RouteMagic

# RouteMagic Console Manager

## RM-CM200 / RM-CM1200

# ユーザーズガイド

- Version 4.0 -

# はじめに

このたびは RouteMagic Console Manager（RM-CM）をお買い上げいただき、まことにありがとうございます。本書は、RM-CM を正しくご利用いただくための手引書です。本書の内容をよくご理解いただき、RM-CM の活用にお役立てください。

本書は、RM-CM ソフトウェア Version 4.0 を前提に記述されています。最新のソフトウェアおよび関連マニュアルは、弊社ホームページから直接ダウンロードしてご利用いただけます。常に、最新バージョンのソフトウェア環境で RM-CM をご利用ください。

http://www.routrek.co.jp

## 本書の目的

本書は、RM-CM をご利用いただくために必要な初期設定の作業を中心に、RM-CM が提供する機能とその利用方法を説明しています。RM-CM の設置、および RM-CM が提供する各種コマンドの詳細に関しては、「RM-CM 取扱説明書」ならびに「RM-CM クイックリファレンス」をご参照ください。

## 関連ドキュメント

RM-CM には、本書のほかに、次のドキュメントが用意されています。

- **RouteMagic Console Manager　RM-CM1200 / RM-CM200　取扱説明書**
  RM-CM の設置とネットワーク機器への接続に必要な情報を記載した、製品添付の説明書です。RM-CM1200 版と RM-CM200 版があります。

- **RouteMagic Console Manager　クイックリファレンス**
  RM-CM が提供するコマンドの機能を記述したハンドブックです。

- **RouteMagic Console Manager　リリースノート**
  最新リリースにおいて追加／変更された機能を中心に記載しています。最新リリースへのアップグレードを行われる際には、必ずリリースノート記載内容を確認の上ご使用ください。

- **RM-CM セットアップサーバ構築・運用ガイド**
  多数の RM-CM を設置される場合の、一括セットアップ／バージョンアップに関して記述しています。

RMC-13-008　03/2007

## ご使用にあたって

（１） 本書の内容については、改良のため予告なしに変更することがあります。

（２） 当製品、および当製品に搭載される弊社が著作権を持つソフトウェアに対して、無断でコピー、逆アセンブル、逆コンパイル、リバースエンジニアリング等を行うことは固くお断りします。

（３） 当製品を海外に持ち出す場合、輸出貿易管理令及び外国為替令に基づくパラメータシート（製品が戦略物資に該当するか否かを判定する該非判定書）を要求されることがあります。パラメータシートを必要とされる場合は、弊社宛ご連絡ください。

# 目次


**1. RM-CM の概要 1**

1.1 RM-CM の設置要件 1
1.2 RM-CM1200 各部の名称と機能 1
1.3 RM-CM200 各部の名称と機能 3

**2. RM-CM の起動 4**

2.1 電源の投入 4
2.2 起動時のステータス確認 4
2.3 IP アドレスの表示 5
2.4 IP アドレス取得失敗時の操作 5

**3. RM-CM の初期設定 7**

3.1 RM-CM へのログイン 7
3.2 特権モードと設定情報の保存 9
3.3 パスワードの設定 10
3.4 ホスト名の変更 11
3.5 ログインユーザの追加 11
3.6 日付と時刻の設定 11
3.7 IP アドレスの手動設定 14

**4. シリアルポートの設定 16**

4.1 RM-CM シェルのコマンドライン操作 19
4.2 ページャの操作 21
4.3 シリアルポートの動作ステータス 21
4.4 COM1～COM12 ポート（監視対象装置接続）の設定 22
4.5 シリアルコンソール接続の機能と設定 22
4.6 モデム接続の機能と設定 24
4.7 PPP 接続のテスト 26
4.8 PPP 接続のカスタム設定 27

**5. 電子メールサービスの設定 28**

5.1 電子メールサービスの設定とサービスの開始 28
5.2 電子メールの送信テスト 30
5.3 電子メールの受信テスト 31

**6. RM-CM 機能の利用と設定 32**

6.1 フィルタ機能の利用とデフォルトフィルタ 33
6.2 監視対象装置の生存確認 34
6.3 監視対象装置とネットワーク関連情報の取得と自動送信 35
6.4 RM-CM の生存確認（キープアライブ）の送信 36
6.5 SNMP エージェントの機能と設定 36

**7. RMS(RouteMagic Server)利用時の設定 39**

7.1 メールポート（ml0）と COM ポート(comN)の設定 39
7.2 セキュリティ関連の設定 40

7.3 フィルタの設定 41
7.4 RMS への RM-CM の登録 41

**8. セキュリティに配慮した運用 42**

8.1 ユーザ名、パスワードの設定 42
8.2 ssh(Secure SHell) の使用 42
8.3 RM-CM に対するアクセス制限の設定 43
8.4 送信メールの暗号化 43

**9. 監視対象装置の操作とログの表示 44**

9.1 監視対象装置との接続 44
9.2 connect 時の操作 44
9.3 監視対象装置との直接接続 45
9.4 透過モードでの接続 46
9.5 直接接続時の操作 46
9.6 接続時の注意 47
9.7 エスケープキャラクタの機能 48
9.8 接続ユーザの制限 48

**10. シリアルポートのログと装置設定情報の表示・保存 49**

10.1 シリアルポートのログ表示 49
10.2 装置設定情報の表示 49
10.3 シリアルポートのログおよび装置設定情報の保存 50

**11. 監視対象装置の電源管理 51**

11.1 電源管理関連の設定 51
11.2 装置の電源の操作 52
11.3 監視対象装置が無応答の場合の自動リブート設定 52

**12. 認証サーバ(RADIUS)対応 53**

12.1 認証方式の設定 53
12.2 RADIUS サーバの設定 53

**13. その他の機能の利用と使用上の注意 54**

13.1 RM-CM の設定の表示と保存 54
13.2 RM-CM の電源のオフとハードウェアリセット 55
13.3 LCD 操作パネルの使用方法（RM-CM1200） 56
13.4 ファンクションスイッチの使用方法（RM-CM200） 60
13.5 telnet/ssh クライアント機能の利用 61
13.6 リモートホストポートへの接続機能 63

**14. 一般機器の接続とフィルタ・スクリプト 64**

14.1 システム組み込みのフィルタ・スクリプト 64
14.2 一般機器の接続要件 64
14.3 一般機器接続時の設定とフィルタ・スクリプトの機能 64
14.4 多機種対応用フィルタ・スクリプトの利用 67

**15. ユーザ定義フィルタの作成 68**

15.1 フィルタの作成と設定 68
15.2 フィルタ設定の確認テスト 69

**16. ユーザ定義スクリプトの作成 71**

16.1 スクリプトの記述 71
16.2 コマンドの機能 72
16.3 装置操作用スクリプトの作成 76
16.4 スクリプトのデバッグ方法 82
16.5 一般機器に対する COM ポートの設定 85
16.6 スクリプト作成上の注意点 86
16.7 よくあるご質問 86

**17. 製品仕様 87**

17.1 本体仕様 87
17.2 COM ポート仕様 87
17.3 付属ケーブル／コネクタ仕様 88

**18. 商標とライセンス 89**

# 1. RM-CM の概要

本章では、RouteMagic Console Manager（以下、RM-CM)に接続する監視対象装置と接続ネットワークに関する要件、および RM-CM1200 と RM-CM200 に装備されるポートの機能を紹介します。RM-CM の設置と監視対象装置との接続に関しては、RM-CM1200、RM-CM200 用として提供される「取扱説明書」をご覧ください。

## 1.1 RM-CM の設置要件

RM-CM は、以下の要件を満たす装置とネットワーク環境に接続してご利用いただけます。

### 監視対象装置要件

- RS-232C/D をコンソールポートとして持つこと。
- コンソールポートが ascii 文字を出力するダム端末（ASCII 端末）として機能すること。
- エラーメッセージ、その他ログをコンソールポートに出力すること。

### RM-CM 接続ネットワーク必須要件

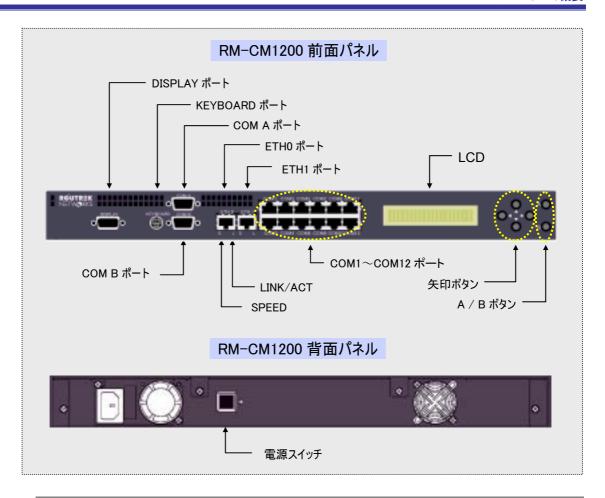
- TCP/IP ネットワーク（IP Version4）であること。
- インターネット上ホストへ SMTP を用いた IP reachable であること。

### RM-CM 接続ネットワーク推奨要件

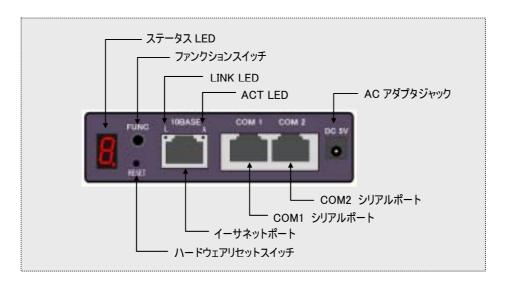
- 正しく設定された DNS サーバへ IP reachable であること。
- メール送受信先の MTA(Mail Transfer Agent)とダイレクトに通信可能であること(リレーホストや POP でのメール受信を使用しないこと)。
- DHCP または RARP サーバが用意されていること。
- NTP サーバが用意されていること
- TFTP サーバが用意されていること(設定の保存、アップグレード用)
- Internet 経由で RM-CM と RMS を接続する場合は、RM-CM－RMS 間通信における認証／暗号化の機能を利用すること。

## 1.2 RM-CM1200 各部の名称と機能

RM-CM1200 は、12 個の監視対象装置接続専用ポート（COM1~COM12）と 2 つのイーサネットポートを装備するモデルです。DISPLAY/KEYBOARD ポート、モデム接続専用ポート等に加えて LCD 操作パネルも装備し、ネットワーク経由のみでなくローカルな操作性にも優れています。

RM-CM1200 に装備されるポートの名称と機能概要は、以下の通りです。

| 名称 | 機能 |
|---|---|
| DISPLAY ポート | ディスプレイ装置接続用ポート （VGA モニタが接続可能） |
| KEYBOARD ポート | キーボード接続用ポート （日本語・英語　PS/2 キーボードが接続可能） |
| COM A　ポート | シリアルコンソール端末接続用ポート<br>（ASCII 端末、PC のターミナルエミュレータが接続可能） |
| COM B　ポート | モデム接続用シリアルポート<br>バックアップ回線用のモデム接続ポート。モデム接続により、イーサネットポートに接続されたネットワークに障害が発生した場合でも、モデム経由のメール送信や機器操作が可能になります。 |
| ETH0　ポート | イーサネットポート （外部ネットワーク接続用）<br>RM-CM からのメール送受信等、外部との通信に使用されます。 |
| ETH1　ポート | イーサネットポート （メンテナンス専用）<br>メンテナンス用に装備されるポート。LAN 内の同一セグメント上に存在するノードに対してのみ通信可能です。DHCP による IP アドレス取得はできません。 |
| LINK/ACT LED | イーサネットリンク/アクト表示用 LED （データ送受信時点滅） |
| SPEED LED | イーサネットスピード表示用 LED （100Mbps　時点灯） |
| COM1～COM12　ポート | シリアルポート （監視対象装置接続用）<br>監視対象とする各種ネットワーク機器のコンソールポートと接続します。 |
| LCD | 各種ステータス、操作メッセージ表示用 LCD 装置<br>LCD 表示とボタンの操作により、RM-CM の操作を行うことができます。 |
| 矢印ボタン | LCD パネル用操作ボタン |
| A　ボタン | 実行ボタン　　（操作の実行確認） |
| B　ボタン | キャンセルボタン （操作のキャンセル） |

# 1.3　RM-CM200 各部の名称と機能

RM-CM200 は、2 個のシリアルポート（COM1,COM2）を装備するモデルです。シリアルポートには、監視対象装置 2 台、または第 2 シリアルポートにシリアル端末またはモデムを接続することが可能です。RM-CM200 に装備されるポートの名称と機能概要は、以下の通りです。

| 名称 | 機能 |
|---|---|
| ステータス LED | RM-CM の動作状態を表示用 LED<br>通常動作時は、RM-CM の IP アドレスが表示されています。 |
| ファンクションスイッチ | RM-CM 操作用スイッチ<br>シャットダウン／リブート機能、各種状態の表示／設定機能を提供します。 |
| LINK LED | イーサネットリンク表示用 LED （10BASE-T のリンクが確立時点灯） |
| ACT LED | イーサネットアクト表示用 LED （10BASE-T のデータ送受信時点滅） |
| COM1 ポート | シリアルポート （監視対象装置接続用）<br>監視対象とする各種ネットワーク機器のコンソールポートと接続します。 |
| COM2 ポート | シリアルポート （監視対象装置、またはシリアル端末/モデム接続用）<br>COM2 ポートに、シリアル端末、あるいはモデムを接続した場合は、COM2 ポートを経由した RM-CM の操作やメールの送信が可能になります。 |
| イーサネットポート | イーサネットポート（外部ネットワーク接続用）<br>RM-CM からのメール送受信等、外部との通信に使用されます。 |
| ハードウェアリセットスイッチ | RM-CM をリブート（再起動）します。シャットダウンは実行されません。 |

# 2. RM-CM の起動

## 2.1　電源の投入

RM-CM の装置とネットワークへの接続が完了したら、RM-CM の電源を投入してください。RM-CM1200 の電源スイッチは、背面パネルにあります。RM-CM200 には、電源スイッチはありません。付属の AC アダプタを電源コンセントに差し込んでください。

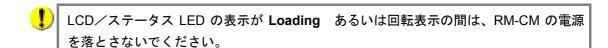
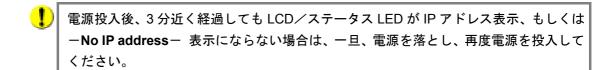
RM-CM の電源を入れて電気的な異常が生じた場合は、速やかに電源を落としてください。

## 2.2　起動時のステータス確認

電源投入後、RM-CM は IP アドレスの取得動作に入ります。この間のステータスは、LCD もしくはステータス LED の表示によって確認します。RM-CM1200/CM200 いずれの機種においても、システムが正常に起動した場合は、LCD/LED に IP アドレス表示、もしくは IP アドレス取得の失敗の通知が表示されます。システムの起動と IP アドレスの取得動作中、LCD/LED の表示は、次のように変化します。

| RM-CM1200 / LCD 表示 | | RM-CM200 / ステータス LED 表示 |
|---|---|---|
| Starting | | 全点灯 |
| | | 内部動作ステータス表示 |
| RM-CM ｿﾌﾄｳｪｱﾊﾞｰｼﾞｮﾝ表示 | | RM-CM ｿﾌﾄｳｪｱﾊﾞｰｼﾞｮﾝ表示 |
| Loading | | 回転表示 |
| アドレス取得時 | IP アドレス表示（ETH0） | IP アドレス表示 |
| 取得失敗時 | **No IP address** 表示 | －no IPAddrESS－ 表示 |

LCD／ステータス LED の表示が **Loading** あるいは回転表示の間は、RM-CM の電源を落とさないでください。

電源投入後、3 分近く経過しても LCD／ステータス LED が IP アドレス表示、もしくは－**No IP address**－ 表示にならない場合は、一旦、電源を落とし、再度電源を投入してください。

## 2.3　IP アドレスの表示

IP アドレスが自動取得された場合、下記のように LCD／ステータス LED に取得された IP アドレスが表示されます。

**RM-CM1200**：　取得された ETH0 ポートの IP アドレスが、下図のように LCD に表示されます。

```
ＥＴＨ０：１９２．１６８．１０．１８５
      RM-CM１２００
```

ETH1 ポートの IP アドレスは、DHCP サーバから自動取得できません。LCD 操作パネル、または RM-CM のコマンドを利用してアドレスの手動設定を行ってください。
➡「3.7　IP アドレスの手動設定」参照

**RM-CM200**　：　取得された IP アドレスは、下図のように、1 文字ずつステータス LED に表示されます。各文字は 1 秒間ずつ表示され、終了文字"－"表示後、再び先頭からの表示が繰り返されます。

例えば"192.168.82.3 / 255.255.255.0 "の表示は次のようになります。

## 2.4　IP アドレス取得失敗時の操作

IP アドレスが自動取得できなかった場合（No IP Address 表示）は、ローカル接続されたシリアル端末、もしくはキーボード／モニタ装置を使用して RM-CM にログインし、IP アドレスの手動設定を行ってください。　➡「3.7　IP アドレスの手動設定」参照

シリアル端末やキーボード・モニタが接続されていない場合は、以下の方法でも IP アドレスの設定を行うことができます。

**RM-CM1200**　：LCD 操作パネルを利用して、IP アドレスを手動設定する。
➡「13.3　LCD 操作パネルの使用方法（RM-CM1200）」参照

**RM-CM200**　：ファンクションスイッチ「４」の機能を利用して、IP アドレスの自動設定を行う。（この機能は、DHCP サーバが用意されていない場合にも使用すること

ができます。）

➡「13.4　ファンクションスイッチの使用方法（RM-CM200）」参照

# 3. RM-CM の初期設定

RM-CM の起動完了後、RM-CM にログインして RM-CM 自身の設定を行います。

## 3.1 RM-CM へのログイン

ログインには LAN 上のホストからネットワークを介して行う方法と、シリアル端末（またはキーボード／モニタ）から行う方法があります。

### ネットワーク経由の接続

RM-CM 起動時に IP アドレスが自動設定された場合は、RM-CM に表示された IP アドレスを使用して、ssh（または telnet）、WEB ブラウザ（WEB インターフェースは RM-CM1200 のみ）で接続してください。

WEB インターフェースで設定可能な各種機能に関しては、➡「RM-CM_WEB インターフェースリファレンス」をご参照ください。

### ローカルコンソールの接続

IP アドレスが未設定の場合は、まず、ローカル接続のコンソール（RM-CM1200 の COMA ポート／RM-CM200 の COM2 ポートに接続されたシリアル端末、もしくは RM-CM1200 に接続されたキーボード／ディスプレイ）から RM-CM にログインする必要があります。シリアル端末、キーボード／ディスプレイの接続に関しては、製品添付の「取扱説明書」をご参照ください。

- **シリアル端末からログインする場合**

  シリアル端末接続時は、接続する端末の端末パラメータを下記の RM-CM デフォルト値に合わせて設定してください。

| パラメータ | デフォルト値 |
|---|---|
| データ転送速度 | 9600 bps |
| キャラクタビット長 | 8 bits |
| パリティチェック | 無し |
| ストップビット長 | 1 bit |
| フロー制御方式 | 無し |

- **モニタ／キーボードを使用する場合**

  **RM-CM1200** の DISPLAY/KEYBOARD 端子にモニタとキーボードを接続してログインする場合、最初にキーボードの種類を尋ねるメッセージが表示されます。
  英語キーボードの場合は“１”を、日本語キーボードの場合は“２”を入力してください。

## ユーザ名とパスワードの入力

いずれの方法で接続した場合も、RM-CM との接続が完了すると、ログインプロンプトが表示されます。以下のユーザ名とデフォルトパスワードを入力して RM-CM にログインします。

| ユーザ名 | パスワード |
| --- | --- |
| rmc | 無し |

# 3.2 特権モードと設定情報の保存

以後に記述する RM-CM の設定操作を行う場合は、下記の点にご注意ください。

## 特権モード

特権モードは、RM-CM の設定や状態を変更する操作を実行するためのモードです。ログイン直後、RM-CM は通常モードになっていますが、このモードではすべてのコマンドを実行することはできません。以後の初期設定操作は、すべて、特権モードに移行してから行います。

特権モードへの移行は、**enable** コマンドの実行によって行います。特権モードへの移行にはパスワードが必要ですが、工場出荷状態ではパスワードは設定されていません。初期設定時に、必ずパスワードの設定を行ってください。

特権モードでのみ実行可能なコマンドを通常モードで実行した場合、"command not found" のエラーが表示されます。

## 設定情報の保存

以後の設定操作によって設定された内容は、RM-CM のメモリに記憶されます。設定情報をリブート後も有効にするためには、**write memory** コマンドを実行して、メモリ内の設定情報をファイルに書き込んでください。

```
myrmc login: rmc
Password:
rmc@myrmc > enable                        ← 特権モードへの移行要求
password:
[rmc@myrmc]#

      ･････ 各種設定コマンド実行 ････

[rmc@myrmc]# write memory                 ← 設定情報の保存要求
This command will overwrite the current startup configuration.
Are you sure ? [y]es/[n]o: y              ← ファイル書き込みの実行確認
ok
[rmc@myrmc]#
[rmc@myrmc]# disable                      ← 通常モードに戻る
rmc@myrmc >
```

以後の記述で利用される各種コマンドの機能と書式、および設定情報のデフォルト値に関しては、➡「RM-CM クイックリファレンス」をご参照ください。

# 3.3　パスワードの設定

RM-CM にログインして設定などの操作をするためには、ログイン、特権モードのそれぞれにパスワードが必要です。工場出荷時にはいずれのパスワードも設定されていませんので、次の操作により任意のパスワードを設定してください。
なお、ログインパスワードはユーザごとに設定されますが、特権モードパスワードは全ユーザに共通となります。

## RM-CM ログインパスワード

RM-CM にログインするためのパスワードを設定します。パスワードの設定／変更は、ユーザごとに **set password** コマンドによって行います。工場出荷時は、”rmc” ユーザのみが設定されています。

```
myrmc login: rmc
Password:
rmc@myrmc > enable                      ← 特権モードへの移行要求
password:                               ← 特権モードパスワード入力
[rmc@myrmc]# set password               ← パスワード設定コマンド実行
Enter new password:                     ← 新しいログインパスワード入力
Re-enter new password:                  ← 同一パスワードの再入力
Password changed
[rmc@myrmc]# disable                    ← 通常モードに戻る
rmc@myrmc >
```

## 特権モードパスワード

特権モードで RM-CM を利用するための全ユーザ共通のパスワードです。パスワードの設定／変更は **set enable-password** コマンドによって行います。特権モードに対するパスワードの設定を行う場合は、旧パスワードの入力が必要とされます。

```
rmc@myrmc > enable                      ← 特権モードへの移行要求
password:                               ← 特権モードパスワード入力
[rmc@myrmc]# set enable-password        ← 特権パスワード設定コマンド発行
current password:                       ← 現在の特権モードパスワード入力
new password:                           ← 新しい特権モードパスワード入力
retype new password:                    ← 同一パスワードの再入力
password changed
[rmc@myrmc]# disable                    ← 通常モードに戻る
rmc@myrmc >
```

## 3.4　ホスト名の変更

工場出荷時には、ホスト名＝myrmc がデフォルト値として設定されています。ホスト名は、**set hostname** コマンドで変更することができます。

以下に、ホスト名を "rmc1" に変更する場合の例を示します。設定されたホスト名は、プロンプト表示に反映されます。また、設定されているホスト名を確認する場合は、**show hostname** コマンドを実行してください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set hostname rmc1              ← ホスト名を"rmc1"に設定
[rmc@rmc1]# show hostname                   ← ホスト名を確認
[rmc@rmc1]# disable
rmc@rmc1 >
```

## 3.5　ログインユーザの追加

工場出荷時には、ユーザ名＝rmc がデフォルト値として設定されています。ユーザ名の追加登録は、**set user-name** コマンドによって行います。登録ユーザを削除する場合は、**set no user-name {*ユーザ名*}** を実行してください。

以下に、ユーザ名"operator1"（パスワードは"passwd"）を追加する例を示します。登録されているユーザ名のリストは、**show user-names** コマンドにより確認できます。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set user-name operator1 passwd   ← ユーザ"operator1"を追加
[rmc@myrmc]# show user-names                  ← 登録ユーザー名を確認
[rmc@myrmc]# disable
rmc@myrmc >
```

## 3.6　日付と時刻の設定

RM-CM は、NTP サーバを利用してシステムクロックを自動的に設定することができます。NTP サーバが利用できない場合は、システムクロックを手動設定する必要があります。

タイムゾーンの設定

工場出荷時の状態では、タイムゾーンとして日本標準時（JST）がデフォルトで設定されています。日本標準時以外の地域で RM-CM を利用される場合は、まずタイムゾーンの設定を行ってください。タイムゾーンは **set timezone** コマンドの引数として指定します。設定可能な引数は、以下の通りです。

| | | | |
|---|---|---|---|
| CST6CDT | (米国中部標準時) | PST8PDT | (米国太平洋標準時) |
| EST5EDT | (米国東部標準時) | UCT | (Universal Coordinated Time) |
| JST | (日本標準時) | GMT | (グリニッジ標準時) |
| KST | (韓国標準時) | GMT±N | |
| MST7MDT | (米国山地標準時) | | |

以下に、タイムゾーンとして米国太平洋標準時を設定する場合の操作例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set timezone PST8PDT          ← タイムゾーンを設定
Thu Jul  4 22:18:37 PDT 2002               ← 設定後の時刻を表示
[rmc@myrmc]# disable
rmc@myrmc >
```

NTP サーバの設定（推奨）

NTP サーバが利用可能な場合は、**set ntp-server** コマンドで NTP サーバ名を指定します。RM-CM のシステムクロックは、NTP サーバからの取得時刻に基づいて定期的に設定されます。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set ntp-server ntp1.jst.mfeed.ad.jp   ← NTP サーバ名を設定
Wed Dec 11 16:16:04 JST 2002                       ← 設定後の時刻を表示
[rmc@myrmc]# disable
rmc@myrmc >
```

## 日付と時刻の手動設定（NTP サーバが利用できない場合）

NTP サーバが利用できない場合は、**set date** コマンドにより、日付と時刻を手動設定してください。以下に 2002 年 12 月 1 日午前 10 時 30 分を設定する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set date 120110302002         ← 日付と時刻の設定
Sun Dec  1 10:30:00 JST 2002               ← 設定後の時刻を表示
[rmc@myrmc]# disable
rmc@myrmc >
```

システムクロックの確認

システムクロックの値は、**show date** コマンドによって確認します。

```
rmc@myrmc> show date
Tue Nov 26 14:47:39 JST 2002               ← 現在のシステムクロックを表示
rmc@myrmc>
```

# 3.7　IP アドレスの手動設定

## ETH0 ポートのアドレス設定 （DHCP／RARP サーバが用意されていない場合）

RM-CM は、ETH0 ポートの IP アドレスを DHCP または RARP サーバから自動的に取得する機能を備えていますが、IP アドレスの自動取得ができない場合や任意のアドレスに設定変更したい場合は、**set address** コマンドによって IP アドレスを手動設定することができます。

設定すべき情報は、IP アドレス、ネットマスク、デフォルトゲートウェイ、ブロードキャストアドレス、およびネームサーバ（DNS）です。デフォルトゲートウェイの設定は省略可能です。

以下に、ETH0 イーサネットポートに IP アドレスを設定する例を示します。

```
rmc@myrmc > enable                                      ← 特権モードへの移行要求
password:                                               ← 特権モード・パスワード入力
[rmc@myrmc]# set port eth0                              ← カレントポートを eth0 に指定
[rmc@myrmc(eth0)]# set name-servers xx.xx.xx.xx yy.yy.yy.yy
                                                        ← ネームサーバ(DNS)の設定
 [rmc@myrmc(eth0)]# set address xx.xx.xx.xx yy.yy.yy.yy zz.zz.zz.zz
                                                        ← IP アドレス、ネットマスク、デフォルト
                                                          ゲートウェイの設定
[rmc@myrmc(eth0)]# set broadcast-address xx.xx.xx.xx
                                                        ← ブロードキャストアドレスの設定
[rmc@myrmc(eth0)]# show port eth0                       ← ポート eth0 の設定を確認
[rmc@myrmc(eth0)]# write memory                         ← 設定情報を設定ファイルに保存
[rmc@myrmc(eth0)]# disable                              ← 通常モードに戻る
rmc@myrmc > quit                                        ← ログアウトする
```

ネットワーク経由でログインして上記の操作を行った場合、**set address** コマンド実行時点で一旦接続が切れてしまいます。設定した IP アドレスに ssh（または telnet）で接続して再度ログインし、以後のコマンドを実行してください。リブートの必要はありません。

## ETH1 ポートのアドレス設定（RM-CM1200 のみ）

RM-CM1200 では、外部ネットワーク接続用のイーサネットポートに加えて、メンテナンス専用のイーサネットポート（ETH1）が装備されています。ETH1 ポートは、通常のイーサネットポートと同様にネットワークに接続して使用することができますが、LAN 内の同一セグメント上に存在するノードに対してのみ通信可能です。

ETH1 ポートの IP アドレスは、DHCP サーバから取得することはできません。当ポートを利用する場合は、**set address** コマンドの実行、もしくは LCD 操作パネルの使用により、IP アドレスの手動設定を行ってください。
LCD 操作パネルの使用方法に関しては、➡「13.3　LCD 操作パネルの使用方法（RM-CM1200）」参照。

ETH1 ポートの設定情報は、IP アドレス、ネットマスク、ブロードキャストアドレスです。それ以外の設定（Ex. デフォルトゲートウェイ）を要求しても受け付けられません。

以下に、set address を実行して ETH1 ポートにアドレスを設定する例を示します。

```
rmc@myrmc > enable                                      ← 特権モードへの移行要求
password:                                               ← 特権モード・パスワード入力
[rmc@myrmc]# set port eth1                              ← カレントポートを eth1 に指定
[rmc@myrmc(eth1)]# set address xx.xx.xx.xx yy.yy.yy.yy
                                                        ← IP アドレス、ネットマスクの設定
[rmc@myrmc(eth1)]# set brodcast-address xx.xx.xx.xx
                                                        ←ブロードキャストアドレスの設定
[rmc@myrmc(eth1)]# show port eth1                       ← ポート eth1 の設定を確認
[rmc@myrmc(eth1)]# write memory                         ← 設定情報を設定ファイルに保存
[rmc@myrmc(eth1)]# disable                              ← 通常モードに戻る
rmc@myrmc > quit                                        ← ログアウトする
```

# 4．シリアルポートの設定

RM-CM には、下表のように RM-CM200 では 2 個、RM-CM1200 では 14 個のシリアルポートが装備されています。RM-CM に対する初期設定が完了したら、com*N* シリアルポートの設定を行ってください。

| 4．シ | COM1～COM12 | 監視対象装置接続用ポート |
|---|---|---|
| | COMA | シリアル端末接続用ポート |

RM-CM には、下表のように RM-CM200 では 2 個、RM-CM1200 では 14 個のシリアルポートが装備されています。RM-CM に対する初期設定が完了したら、com*N* シリアルポートの設定を行ってください。

| RM-CM1200 | | |
| --- | --- | --- |
| RM-CM200 | COM1 | 監視対象装置接続用ポート |
| | COM2 | 監視対象装置／シリアル端末／モデム接続用ポート |

**RM-CM200** の COM2 ポートには、監視対象装置／シリアル端末／モデムのいずれかを接続することができますが、工場出荷時のデフォルト設定はシリアル端末接続です。また、COM1 は、監視対象装置接続専用ポートとなります。

## 4.1 RM-CM シェルのコマンドライン操作

コマンド入力の際には、以下のような補助機能が用意されているのでご活用ください。

- **簡易ヘルプの表示**：

  コマンドライン入力中に'?'を入力すると、その時点で入力可能なコマンドが引数の簡易説明とともに表示されます。

  例:

```
[rmc@myrmc]# show h?
        show hostname
        show hosts
```

- **コマンド文字列の補完表示**：

  コマンドの入力中に TAB キーを押すと、入力済みの文字列から推測されるコマンド名を保管して表示します(なお、引数部分は補完されません)。

  例:

```
[rmc@myrmc] # w
→TAB キーを入力
[rmc@myrmc]# write

[rmc@myrmc]# write m
→TAB キーを入力
[rmc@myrmc]# write memory
```

- **コマンド文字列の自動補完**：

  コマンドの入力中に ENTER キーを押した場合、その時点で推測されるコマンド名を自動的に保管して実行します。
  例として、"**wrm**"と入力し ENTER キーを押すと、**write memory** コマンドが実行されます。

  また、推測されるコマンドが複数ある場合、コマンドを実行する代わりに候補となるコマンドを表示します(なお、引数部分は補完されません)。

- **入力ヒストリの表示**：

- **RM-CM シェルのショートカットキー一覧**：

| キー | 機能 |
|---|---|
| Enter | 入力したコマンドを実行する。<br>途中までコマンド入力した状態で Enter を入力した場合、自動的に補完して実行される。<br>例） "show run" 入力後 Enter キーで、"show running-config" を実行。<br>但し、複数のコマンドに一致する場合は、該当するコマンドの一覧を表示する。 |
| Ctrl－I<br>Tab | 途中まで入力したコマンド名を補完して表示する。<br>（引数部分は補完の対象外）<br>例） "ena"入力後 Tab キーで"enable" を表示。 (実行はしない) |
| ？ | 簡易ヘルプを表示する。<br>途中までコマンド入力した状態で"？"を入力した場合、その時点で可能性のあるコマンドを表示する。<br>例）"set ?" で set で始まるコマンドの簡易ヘルプをすべて表示。 |
| Ctrl－B, ← | カーソルを 1 つ左に移動 |
| Ctrl－F, → | カーソルを 1 つ右に移動 |
| Ctrl－A | 行の先頭にカーソルを移動 |
| Ctrl－E | 行の末尾にカーソルを移動 |
| Ctrl－D | カーソル位置の文字を 1 文字削除 |
| Ctrl－H<br>BackSpace | カーソル左の文字を 1 文字削除 |
| Ctrl－K | カーソル位置から行末までを削除 |
| Ctrl－C | 入力を取り消す。 |
| Ctrl－U | 入力行を全て削除 |
| Ctrl－P, ↑ | 1 つ前のヒストリ（実行したコマンドの履歴）を表示 |
| Ctrl－N, ↓ | 1 つ後のヒストリ（実行したコマンドの履歴）を表示 |
| Ctrl－Z | カレントポートの指定を解除する。 |

## 4.2　ページャの操作

show コマンドの実行時など、1 画面に収まらない内容が表示される場合はページャが起動され、1 画面おきの表示や文字列検索などが可能になります。ページャが起動された場合には、以下の例のように画面最下行に":"が表示されます。スペースで次画面、'**q**'で表示を終了しコマンドラインに戻ります。

以下に、ページャの操作キー一覧を示します。

| キー | 機能 |
|---|---|
| g, < | 行数を入力後このコマンドで指定された行へジャンプ。<br>行数入力が無い場合はファイルの先頭へジャンプ。 |
| G, > | 行数を入力後このコマンドで指定された行へジャンプ。<br>行数入力が無い場合はファイルの最後行へジャンプ。 |
| p | 指定パーセント(0～100)位置にジャンプ。<br>ただしバイト数ではなく、行数で計算。 |
| b, Ctrl－b | 前のページに戻る。 |
| u, Ctrl－u | 前の半ページに戻る。 |
| k / y, Ctrl－k / y / p | 前の行に戻る。 |
| j / e, Ctrl－j / e / n, CR | 次の行に進む。 |
| d, Ctrl－d | 次の半ページに進む。 |
| f, Ctrl－f / v, SP | 次のページに進む。 |
| /<string> | 文字列の前方検索 |
| ?<string> | 文字列の後方検索 |
| n | 前方検索を繰り返す。 |
| N | 後方検索を繰り返す。 |
| q, Q | 表示の終了 |

## 4.3　シリアルポートの動作ステータス

*comN* シリアルポートは、各ポートの利用状態に適した動作を実行するため、以下のコマンドによるステータス管理が行われます。

RM-CM200 において、COM2 ポートに接続される装置を変更した場合（例えば、シリアル端末が接続されていたポートに監視対象装置を接続する場合）は、ポートステータスの変更が必要になりますのでご注意ください。

**set [no] exec** ：当該ポートを RM-CM のコンソールとして使用可能とする／使用不可とする。

（RM-CM200 の COM2、RM-CM1200 の COMA に対してのみ指定可能。）

**set [no] modem**：ポートにモデムを接続して使用する／モデムを接続しない。

（RM-CM200 の COM2、RM-CM1200 の COMB に対してのみ指定可能。）

## 4.4　COM1～COM12 ポート（監視対象装置接続）の設定

監視対象装置のコンソールポートと接続される COM1～COM12 ポートは、工場出荷時に下記のデフォルト値が設定されています。接続する監視対象装置のシリアルポートの設定が以下の値と異なっている場合は、*comN* ポートの設定を適切な値に変更してください。

| パラメータ | デフォルト値 |
|---|---|
| データ転送速度 | 9600　bps |
| キャラクタビット長 | 8 bits |
| パリティチェック | 無し |
| ストップビット長 | 1 bit |
| フロー制御方式 | 無し |

以下にデフォルト値を例にとり、COM1 ポートのパラメータを設定する方法を示します。設定可能な値、および各コマンド機能の詳細に関しては、➡「RM-CM クイックリファレンス」をご参照ください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1                    ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set speed 9600             ← 通信速度の設定
[rmc@myrmc(com1)]# set csize 8                ← 1文字のビット数の設定
[rmc@myrmc(com1)]# set parity none            ← パリティの設定
[rmc@myrmc(com1)]# set stopbits 1             ← ストップビット長の設定
[rmc@myrmc(com1)]# set flowcontrol none       ← フロー制御方式の設定
[rmc@myrmc(com1)]# show port com1             ← com1 の設定を確認
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

RM-CM200 をご利用の場合：

COM2 ポートに監視対象装置を接続する際には、**set no exec** コマンドを実行して、コンソール使用不可の状態に設定変更してください。

## 4.5　シリアルコンソール接続の機能と設定

RM-CM1200 の COMA ポート、RM-CM200 の COM2 ポートは、工場出荷時には下記のデフォルト値が設定され、シリアル端末を接続して RM-CM のローカルコンソールとして利用できる状態（set exec）となっています。

| パラメータ | デフォルト値 |
|---|---|
| データ転送速度 | 9600 bps |
| キャラクタビット長 | 8 bits |
| パリティチェック | 無し |
| ストップビット長 | 1 bit |
| フロー制御方式 | 無し |

set exec が設定された状態では、端末パラメータは、データ転送速度のみが任意に設定可能です。また、当該ポートに対して set exec を実行した場合、データ転送速度を除く端末パラメータは上記の値に再設定されます。

## 端末パラメータの設定

以下に、RM-CM200 の COM2 ポートの端末パラメータを変更する場合の例を示します。RM-CM1200 では、カレントポートを "**coma**" として同様の操作を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2                    ← カレントポートを com2 に指定
[rmc@myrmc(com2)]# set speed 38400            ← 通信速度を 38400bps に設定
[rmc@myrmc(com2)]# show port com2             ← com2 の設定を確認
[rmc@myrmc(com2)]# disable
rmc@myrmc >
```

## シリアルコンソール接続の禁止

RM-CM200 の COM2 ポート、RM-CM1200 の COMA ポートは、デフォルト状態ではローカルコンソール用のポートとして機能しますが、**set no exec** を実行して、コンソールとしての使用を禁止することも可能です。

以下に、COMA ポートの設定を変更する例を示します。RM-CM200 の COM2 ポートに監視対象装置を接続する場合、および COM2 ポートのローカルコンソールとしての使用を禁止する場合も、カレントポートを "**com2**" として同様の設定を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port coma                    ← カレントポートを comA に指定
[rmc@myrmc(coma)]# set no exec                ← シリアルコンソールの使用停止
[rmc@myrmc(coma)]# disable
rmc@myrmc >
```

設定変更を行うポートに接続されたシリアル端末から set no exec を実行した場合、コマンド実行完了直後からこのポートへのアクセスが不可となりますのでご注意ください。

### シリアルコンソール接続に戻したい場合

COMA ポートや COM2 ポートをローカルコンソールとして使用可能な状態に戻したい場合は、ネットワーク経由で RM-CM にログインして **set exec** コマンドを実行します。

監視対象装置やモデムの接続されていた RM-CM200 の COM2 ポートにシリアル端末を接続してローカルコンソールとして使用する場合も同様の操作が必要です。

以下に、RM-CM200 の COM2 ポートをローカルコンソール接続の状態に戻す場合の操作例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2                ← カレントポートを com2 に指定
[rmc@myrmc(com2)]# set exec               ← シリアルコンソール接続の指定
[rmc@myrmc(com2)]# disable
rmc@myrmc >
```

## *4.6　モデム接続の機能と設定*

RM-CM が利用しているイーサネットに異常が発生した場合でも、RM-CM1200 の COMB ポート、あるいは RM-CM200 の COM2 ポートにモデムを接続しておくことにより、バックアップのアクセス手段を確保することができます。COMB または COM2 ポートにモデム接続の設定（set modem）が行われていると、RM-CM はイーサネットポートからのメール送信に異常が発生した場合、自動的に PPP 接続を実行してモデム経由でメールを送信します。また、無手順接続や PPP 接続で遠隔地から RM-CM にログインして機器操作を行うことも可能になります。

### COMB / COM2 ポートの設定

モデム接続機能を利用する場合は、COM B / COM2 ポートに対する端末パラメータの設定、および **set modem** コマンドの実行が必要です。このコマンドは、モデムの種類を指定すると同時に、当該ポートにモデムが接続されていることを RM-CM に通知します。

COM B / COM2 ポートのデフォルト設定は以下の値となっており、データ転送速度のみが任意に設定可能です。データ転送速度のデフォルト値は、RM-CM1200 と RM-CM200 で異なりますのでご注意ください。

| パラメータ | デフォルト値 | |
|---|---|---|
| データ転送速度 | RM-CM1200/COMB | 38400　bps |
| | RM-CM200/COM2 | 9600　bps |
| キャラクタビット長 | 8 bits | |
| パリティチェック | 無し | |
| ストップビット長 | 1 bit | |
| フロー制御方式 | 無し　　※ | |

※　“set modem”時は hardware

以下に、RM-CM1200 の COMB に設定された通信速度を 115200bps に変更した後、モデム名の指定とモデム接続の通知を行う場合の例を示します。RM-CM200 の COM2 にモデムを接続する場合も、設定対象のポートに COM2 を指定して、同様の操作を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port comb                  ← カレントポートを comB に指定
[rmc@myrmc(comb)]# set speed 115200         ← 通信速度を 115200bps に設定
[rmc@myrmc(comb)]# set modem generic        ← モデム名指定とモデム接続の通知
[rmc@myrmc(comb)]# show port comb           ← comB の設定を確認
[rmc@myrmc(comb)]# disable
rmc@myrmc >
```

RM-CM で使用可能なモデム名、動作確認済みのモデム等に関しては、➡「RM-CM リリースノート」をご参照ください。

## PPP 接続の設定

COM B / COM2 ポートに対する端末パラメータの設定を行った後、**set ppp-username** コマンドにより RM-CM が PPP 接続するアクセスポイントの指定を行います。設定に必要な情報は、ユーザ名、パスワード、およびアクセスポイントの電話番号です。

以下に、RM-CM1200 の COMB ポートに対して、ユーザ名 : rmcuser、パスワード : routrek、電話番号 : 111-222-3456 を設定する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port comb                        ← カレントポートを comB に指定
[rmc@myrmc(comb)]# set ppp-username rmcuser routrek 1112223456
                                                  ← PPP 接続情報を設定
[rmc@myrmc(comb)]# show port comb                 ← PPP の設定内容を表示
[rmc@myrmc(comb)]# disable
rmc@myrmc >
```

RM-CM に対して PPP 接続を行う(RM-CM 側を PPP サーバにする)場合には、**set ppp-server** コマンドを実行して、PPP 接続時の RM-CM の PPP アドレスと接続先の PPP アドレスを指定する必要があります。

以下に、RM-CM1200 の COMB ポートに対して RM-CM の PPP アドレス: 192.168.0.1、接続先の PPP アドレス:192.168.0.2 として設定する場合の例を示します。

```
rmc@myrmc> enable
password:
[rmc@myrmc]# set port comb                          ← カレントポートを comB に指定
[rmc@myrmc(comb)]# set ppp-server 192.168.0.1 192.168.0.2
                                                    ← PPP 接続情報を設定
[rmc@myrmc(comb)]# disable
rmc@myrmc>
```

RM-CM に対して PPP 接続を行う場合、PPP 接続の際の ID・パスワードは、RM-CM のログインユーザー名・パスワードを指定してください。

## PPP 接続時の LCD／ステータス LED 表示

PPP 接続時は､LCD あるいはステータス LED に PPP ポートの IP アドレスが表示されます。この表示は、RM-CM が PPP 接続を行った場合に表示されます。RM-CM に対して PPP 接続が行われた場合は、LCD/ステータス LED への表示は行われません。

**RM-CM1200**： LCD に、PPP 接続ポートの IP アドレスが表示されます。

```
ＰＰＰ：１９２．１６８．０．１
    RM-CM１２００
```

**RM-CM200** ： ステータス LED に、下図の形式で IP アドレスが表示されます。

# 4.7 PPP 接続のテスト

PPP 接続の設定を確認するため、手動で PPP 接続を開始する事ができます。

以下に、**ppp-on** コマンドによって PPP 接続を開始し、**traceroute** コマンドによる経路設定の確認と PPP 関連ログの表示を行った後、PPP 接続を終了する場合の例を示します。

```
rmc@myrmc > enable
password：
[rmc@myrmc]# ppp-on                              ← PPP 接続の開始
[rmc@myrmc]# traceroute www.routrek.co.jp        ← 経路設定の確認
[rmc@myrmc]# show port comb                      ← PPP 接続ステータスを表示
[rmc@myrmc]# show log ppp 20                     ← PPP 関連のログを 20 行表示
[rmc@myrmc]# ppp-off                             ← PPP 接続の終了
[rmc@myrmc]# disable
rmc@myrmc >
```

2 分間通信が無い場合、PPP 接続は自動的に終了します。

## 4.8　PPP 接続のカスタム設定

オプション設定によって、PPP 接続時のリトライ回数などのカスタム設定が可能です。

以下に、**set options** コマンドによってメールを最初から PPP 経由で送信する設定にし、PPP のリトライ回数を 9 回、リダイアル間隔を 60 秒に設定する場合の例を示します。

```
rmc@myrmc > enable
password：
[rmc@myrmc]# set options pppmail                 ← メールを PPP 経由で送信する
[rmc@myrmc]# set options pppretry=9,60           ← PPP のリトライ回数・間隔を設定
[rmc@myrmc]# disable
rmc@myrmc >
```

# 5. 電子メールサービスの設定

RM-CM は、監視対象装置から出力されたコンソールメッセージを、メールポートの設定に従って電子メールで指定の宛先に送信します。メールポートは、RM-CM1200 では 0（ml0）から 15（ml15）まで、RM-CM200 では 0（ml0）から 7（ml 7）までが用意されており、各メールポートごとに宛先やフィルタ規則を設定して、必要に応じた送信先や送信内容を指定することができます。以下の記述に従って、メールポートの設定を行ってください。

> メールポート 0（ml0）は、RMS（RouteMagic Server）との通信用にリザーブされています。RMS をご利用の場合、ユーザの任意な利用はできませんのでご注意ください。

> 電子メールサービスは，デフォルトでは停止されています。メールポートの設定完了後、必ず、**set mail-service** コマンドを実行して電子メールサービスを有効にしてください。

## 5.1 電子メールサービスの設定とサービスの開始

### メールの送信単位

RM-CM は、指定の COM ポートから入力されたコンソールメッセージを、一定の行数または文字数(メールポートバッファ長)ごとに電子メール(メールサブジェクト:"Target message")で指定の宛先に送信します。また、一定時間（送信タイマ値）未入力状態が続いた場合は、それまでに受信した文字列を 1 つのメールメッセージとして送信します。

バッファ長およびタイマ値のデフォルト設定は下記の通りです。

| パラメータ | デフォルト値 |
|---|---|
| メールポートのバッファ長 | 64,000 文字、10,000 行 |
| 送信タイマ値 | 10 秒 |

> メールポートのバッファ長の設定を極端に小さくすると、多量のメールが送信される恐れがありますのでご注意ください。

### メール送信先の指定

メールの送信先は、**set mailto** コマンドによってメールポートごとに設定します。

> アドレス設定の誤りなどによりメール送信にエラーが発生した場合、デフォルト状態では、エラーメールは RM-CM 宛てに返信されます。

## COM ポートとの接続

どの COM ポートから入力されたメッセージをどのメールポートに接続して送信するかの設定は、**set spy** コマンドによって設定します。set spy コマンドの設定によって、複数の COM ポートから入力されたメッセージを 1 つの宛先に送信することも可能ですし、1 つの COM ポートから入力されたメッセージを複数の宛先に送信することもできます。

### ■ メールポートの設定例

以下に、COM1 ポート（com1）に接続された監視対象装置からの出力をメールポート 1（ml1）に設定された宛先に送信する例を示します。この例では、メール送付先として someone@routrek.co.jp を、1 メールメッセージの最大文字数、最大行数、送信タイマ値を各々20000 文字、300 行、60 秒に設定しています。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port ml1                                ← カレントメールポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto someone@routrek.co.jp       ← メール送付先アドレスを設定
[rmc@myrmc(ml1)]# set max-nmr-of-chars 20000             ← メールの最大文字数を設定
[rmc@myrmc(ml1)]# set max-nmr-of-lines 300               ← メールの最大行数を設定
[rmc@myrmc(ml1)]# set inactivity-timer 60                ← 送信タイマ値を設定
[rmc@myrmc(ml1)]# show port ml1                          ← メールポート 1 の設定を確認
[rmc@myrmc(ml1)]# set spy com1 ml1                       ← com1 をメールポート 1 に接続
[rmc@myrmc(ml1)]# show spy                               ← 接続設定を確認
[rmc@myrmc(ml1)]# set mail-service                       ← メールサービスの開始
[rmc@myrmc(ml1)]# disable
rmc@myrmc >
```

### ■ メールポートの設定例（複数の送信先を指定する場合）

１つの COM ポートに対して複数の送信先を指定する場合は、複数のメールポートを使用して各々にメールアドレスを設定し、**set spy** コマンドで com*N* ポートと接続します。以下に、COM1 のメッセージをメールポート 1 および 2 に送信する場合の例を示します。メールメッセージの最大文字数／行数と送信タイマ値は、メールポートごとに設定可能です。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port ml1                                ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto someone@routrek.co.jp       ← メール送付先アドレスを設定
[rmc@myrmc(ml1)]# set port ml2                           ← カレントポートを ml2 に変更
[rmc@myrmc(ml2)]# set mailto foo@routrek.co.jp           ← メール送付先アドレスを設定
[rmc@myrmc(ml2)]# show port ml1 ml2                      ← メールポート 1,2 の設定を確認
[rmc@myrmc(ml2)]# set spy com1 ml1                       ← com1 をメールポート 1 に接続
[rmc@myrmc(ml2)]# set spy com1 ml2                       ← com1 をメールポート 2 に接続
[rmc@myrmc(ml2)]# show spy                               ← 接続設定を確認
[rmc@myrmc(ml2)]# set mail-service                       ← メールサービスの開始
[rmc@myrmc(ml2)]# disable
rmc@myrmc >
```

■ **メールポートの設定例（複数 COM ポートのメッセージを 1 つの宛先に送信する場合）**

複数の COM ポートから入力されたメッセージを 1 つのメールアドレスに送信する場合は、各 COM ポートを **set spy** コマンドで 1 つのメールポートに接続します。以下に、COM1 と COM2 からの入力をメールポート ml1 から送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port ml1                          ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto someone@routrek.co.jp  ← メール送付先アドレスを設定
[rmc@myrmc(ml2)]# show port ml1                     ← メールポート 1 の設定を確認
[rmc@myrmc(ml2)]# set spy com1 ml1                  ← com1 をメールポート 1 に接続
[rmc@myrmc(ml2)]# set spy com2 ml1                  ← com2 をメールポート 1 に接続
[rmc@myrmc(ml2)]# show spy                          ← 接続設定を確認
[rmc@myrmc(ml2)]# set mail-service                  ← メールサービスの開始
[rmc@myrmc(ml2)]# disable
rmc@myrmc >
```

フィルタ機能を利用する場合に必要な設定に関しては、下記をご参照ください。

➡「6.1　フィルタ機能の利用とデフォルトフィルタ」
➡「15.　ユーザ定義フィルタの作成」

## *5.2　電子メールの送信テスト*

メールの宛先の設定が正しく行なわれたかどうかは、**mail-test** コマンドによって実際にテストメールを送信して確認することができます。

以下にメールポート ml1 にテストメールを送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# mail-test ml1              ← メールポート ml1 にテストメールを送信
[rmc@myrmc]# show log mail 20           ← メール送信ログを 20 行表示
[rmc@myrmc]# disable
rmc@myrmc >
```

メールポートの設定が正しく行われている場合、上記の操作を実行するとメールポート ml1 に指定された宛先には、以下の内容のメールが送信されます。

---

From: rmc@[*RM-CM の IP アドレス*]
Subject : ml1(0001) : RMC message
This is a test mail from RMC port ml1.

---

テストメールが届かない場合は、**show running-config** コマンドで RM-CM の設定を確認するとともに、**show log mail** および **show log rmc** コマンドでメール送受信ログや、システムログの内容を調べてください。

また、メールポートの設定にエラーがある場合、RM-CM 自身にエラーメールが返信されている場合があります。RM-CM が受信したメールの内容を、下記の **show mail** コマンドにより確認してください。

**mail-test** コマンドは、メールサービスが停止されている場合でも有効です。

PPP 接続によるメール送信テストを行う場合は、**ppp-on** コマンドを実行してからテストメールを送信してください。

## 5.3 電子メールの受信テスト

テストメールが届かなかった場合や、RMS(RouteMagic Server)から RM-CM に送信されたメールが正しく受信できたかどうかの確認など、RM-CM が受信したメールを参照したい場合は、以下のように、**show mail** コマンドを実行します。このコマンドは、RM-CM が最後に受信したメールの詳細情報を表示します。

```
rmc@myrmc >show mail                              ← RMC の最新受信メールを表示
From MAILER-DAEMON   Fri Nov 29 18:03:05 2002
Return-Path: <>
Delivered-To: root@[192.168.10.116]
・・・・・・・   受信メール内容表示（以後省略）・・・・・・・
ok
rmc@myrmc >
```

過去の履歴も含めて、RM-CM が送受信したメールのログを参照したい場合は、**show log mail** コマンドを実行してください。show log mail では、RM-CM のメールログを最新のものから指定行数分表示することができます。

```
rmc@rmc185> show log mail 3                       ← RMC のメールログを表示
Dec 13 18:06:58 rmc185 : 439FC5B7: message-id=<20021213090658.439FC5B7@rmc185>
Dec 13 18:06:58 rmc185 : 439FC5B7: from=<rmc@[192.168.10.185]>, size=1565, nrcpt
=1 (queue active)
Dec 13 18:06:58 rmc185 : 439FC5B7: to=<nwadmin@routrek.co.jp>, relay=mail.rout
rek.co.jp[192.168.10.1], delay=0, status=sent (250 2.0.0 gBD96wB16145 Message a
ccepted for delivery)
ok
rmc@myrmc >
```

# 6. RM-CM 機能の利用と設定

RM-CM は、基本となるメール発信機能に加えて、監視対象装置のコンソールメッセージから必要な情報のみを抽出する機能や、装置からの自動的情報取得など各種の機能を提供します。以下の機能は、“フィルタ”と“スクリプト”を利用して実装され、監視対象装置の種類（装置種別：target-type）ごとに、装置に対して実行すべき操作を定義します。

- **コンソールメッセージのフィルタリング**
  フィルタの設定により、監視対象装置が出力したコンソールメッセージから特定の文字列を含むもののみを抽出して、指定のメールポートに送信することができます。
- **監視対象装置の生存確認**
  監視対象装置が正常に動作中であるか否かを定期的にチェックし、状態に変化があった場合は、指定のメールポートに通知します。
- **監視対象装置とネットワーク関連情報の自動送信**
  監視対象装置にコマンドを発行することによって定期的に情報を収集し、指定のメールポートにこの情報を送信します。また、収集した装置関連情報を RM-CM 内部に保存します。
- **RMS からの要求による監視対象装置へのコマンド発行**
  RMS から受信された監視対象装置に対するコマンド発行要求を処理し、結果を RMS に送信します。

監視対象装置が Cisco 社製品（ルータ、スイッチ、IOS スイッチ）の場合は、デフォルトの設定値が事前に定義されています。したがって、各機能を利用する際に装置の種別やフィルタ・スクリプトを定義する必要はありません。本章の記述に従って、必要な設定を行ってください。

RMC Version3.5 からは、Cisco 以外の装置用フィルタ・スクリプトが最初から用意されています。詳細に関しては、「14. 一般機器の接続とフィルタ・スクリプト」をご参照ください。

Cisco 社製品以外の装置（一般機器）を監視対象とする場合は、下記の記述を参照して装置の種別とフィルタ・スクリプトの設定を行ってください。

➡「14. 一般機器の接続とフィルタ・スクリプト」
➡「15. ユーザ定義フィルタの作成」
➡「16. ユーザ定義スクリプトの作成」

**旧リリースをご利用の方へ**

RMC ソフトウェア Version2.1 以上のフィルタ(tfl0－tfl7)とスクリプトは、装置種別（target_type）ごとに設定する形式に変更されています。従来の形式のフィルタ（fl0－fl7）およびスクリプトもそのままご利用にできますが、設定の詳細に関しては、RMC Version2.0 のマニュアルをご参照ください。

## 6.1 フィルタ機能の利用とデフォルトフィルタ

RM-CM のフィルタは、装置種別ごとに 8 種類（tfl0〜tfl7）を設定することができます。装置種別 “cisco” のフィルタ 0〜3（tfl0〜tfl3）には、Cisco 社製ルータ・スイッチのメッセージ形式に適合するフィルタがデフォルトとして事前に設定されています。

これらのフィルタを利用する場合は、**set spy** コマンドによって COM ポートごとに、送信先メールポートを設定すると同時に適用するフィルタを指定します。複数のフィルタとメールポートを利用して、1 つの COM ポートからの入力を別々のフィルタを使用して送信することも可能です。（フィルタのユーザ定義に関しては、➡「15. ユーザ定義フィルタの作成」参照）

以下に、COM1 に接続された Cisco 装置のコンソールメッセージをフィルタリングして ml1 と ml2 から送信する例を示します。この例では、メールポート 1（ml1）にはフィルタ tfl0 を、メールポート 2（ml2）にはフィルタ tfl1 を設定しています。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1                      ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set target-type cisco        ← com1 ポートの装置種別を cisco に設定
[rmc@myrmc(com1)]# set port ml1                      ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto adr01@routrek.co.jp     ← ml1 のメールアドレスを設定
[rmc@myrmc(ml1)]# set port ml2                       ← カレントポートを ml2 に指定
[rmc@myrmc(ml2)]# set mailto adr02@routrek.co.jp     ← ml2 のメールアドレスを設定
[rmc@myrmc(ml2)]# set spy com1 tfl0 ml1              ← com1 に接続するメールポートと
[rmc@myrmc(ml2)]# set spy com1 tfl1 ml2                 フィルタを設定
[rmc@myrmc(ml2)]# show port com1                ← com1 の設定を確認
[rmc@myrmc(ml2)]# set mail-service              ← メールサービスの開始
[rmc@myrmc(ml2)]# disable
rmc@myrmc >
```

### デフォルトフィルタ仕様

Cisco 装置用のデフォルトフィルタは、ルータ・スイッチからのコンソールメッセージを重要度（メッセージ内の Severity Levels）別に分類して送信する機能を提供します。各デフォルトフィルタと対応する Severity Levels は下表の通りです。上記の設定例では、ml1 にはすべてのエラーメッセージが、ml2 には重要度：High のメッセージのみが送信されます。

| デフォルトフィルタ | エラーメッセージ内の Severity Levels | |
|---|---|---|
| tfl0（重要度:全て） | 0－7　All | 全てのエラーメッセージを通知 |
| tfl1（重要度:High　0－2） | 0－emergency | システム使用不可状態の通知 |
| | 1－alert | 直ちに対処が必要 |
| | 2－critical | 重大な問題の発生を通知 |
| tfl2（重要度:Middle 3－5） | 3―error | エラー状態通知 |
| | 4－warning | 警告状態通知 |
| | 5－notification | 正常だが重要な状態通知 |
| tfl3（重要度:Low 6－7） | 6―informational | 情報通知メッセージ |
| | 7―debugging | デバッギング時のみ発生 |

以下の場合、該当 COM ポートに対するメッセージのフィルタリング処理は、一時的に停止されます。

- connect コマンドによる装置の手動操作中
- スクリプトの実行中(RM-CM が装置にコマンドを投入中)

## *6.2　監視対象装置の生存確認*

RM-CM は監視対象装置の動作状態を定期的にチェックして異常の発生を通知する、生存確認の機能を提供します。この機能は、デフォルトでは停止されています。生存確認を行う場合は、**set target-check** コマンドを使用して生存確認機能を有効にしてください。

生存確認時に監視対象装置が無応答であった場合､RM-CM は指定の宛先にに電子メール（メールサブジェクト："Target not respond"）を送信し、異常の発生を通知します。このメールは、RM-CM が最初に装置の無応答を検知した時点で送信され、応答の復旧が確認された時点で復旧通知（メールサブジェクト：“Target responds”）が送信されます。

生存確認の通知メールは、**set spy** コマンドによって ***targetN*** ポート（*comN* に対応する仮想ポート）に接続されたメールポートから送信されます。デフォルトのメールポートとしては、ml0 が設定されています。

以下に、COM1 ポートに接続された Cisco 社製ルータの生存確認を実行し、状態確認の結果をメールポート 1（ml1）に送信する場合の例を示します。Cisco 製品以外の装置を監視対象とする場合には、予め装置種別をユーザ定義して必要なスクリプトの設定を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1                  ← カレントポートを com1 に設定
[rmc@myrmc(com1)]# set target-type cisco    ← 監視対象装置の種別を Cisco に設定
[rmc@myrmc(com1)]# set target-check         ← 監視対象装置の生存確認を行う
[rmc@myrmc(com1)]# set spy target1 ml1      ← 生存確認送信先ﾒｰﾙﾎﾟｰﾄを設定
[rmc@myrmc(com1)]# show port com1           ← com1 の設定を確認
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

## 6.3 監視対象装置とネットワーク関連情報の取得と自動送信

RM-CM は、監視対象装置から定期的に情報を収集し、内部に保存すると共に、電子メール(メールサブジェクト：“Network information”) で送信する機能を備えています。この機能を有効にするには、**set network-info-time** コマンドによる情報送信時刻の設定、および監視対象装置に対するログインパスワード／特権モードパスワードの設定が必要です。

装置から収集された情報は、**set spy** コマンドによって ***targetN*** ポート（*comN* に対応する仮想ポート）に接続されたメールポートから送信されます。デフォルトのメールポートとしては、ml0 が設定されています。

以下に、COM1 ポートに接続された Cisco ルータを監視対象として、ログインパスワードを key1、特権モードパスワードを key2 とし、ネットワーク情報を午前 8 時 0 分と午後 6 時 0 分の 1 日 2 回、メールポート 1（ml1）に設定された宛先に送信する例を示します。Cisco 以外の製品を監視対象とする場合には、予め装置種別をユーザ定義して必要なスクリプト設定を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1                  ← カレントポートを com1 に設定
[rmc@myrmc(com1)]# set target-type cisco    ← 監視対象装置の種別を Cisco に設定
[rmc@myrmc(com1)]# set target-login-password key1
                                            ← ルータのログインパスワードを設定
[rmc@myrmc(com1)]# set target-enable-password key2
                                            ← ルータの特権モードパスワードを設定
[rmc@myrmc(com1)]# set network-info-time 08,18 0
                                            ← ネットワーク情報送信時刻の指定
[rmc@myrmc(com1)]# set spy target1 ml1      ← ﾈｯﾄﾜｰｸ情報送信先ﾒｰﾙﾎﾟｰﾄを設定
[rmc@myrmc(com1)]# show port com1           ← com1 の設定を確認
[rmc@myrmc(com1)]# set mail-service         ← メールサービスの開始
[rmc@myrmc(com1)]# disable
myrmc >
```

## 6.4　RM-CM の生存確認(キープアライブ)の送信

RM-CM は、RM-CM 自身の動作状態を通知するため、設定情報の一部やログインユーザの履歴、動作に関する各種ログを、電子メール（メールサブジェクト：”RMC keep-alive”）で送信する機能を備えています。この機能はデフォルトで有効になっており、電子メールサービスを開始すると送信が開始されます。送信時刻のデフォルト値は、各 RM-CM に固有の値になっていますが、**set keep-alive-time** コマンドにより任意の時刻に設定可能です。

RM-CM のキープアライブ情報は、**set spy** コマンドによって ***rmc*** ポートに接続されたメールポートに送信されます。デフォルトのメールポートとしては、ml0 が設定されています。

以下に、キープアライブ情報を午前 9 時 0 分と午後 5 時 0 分の 1 日 2 回、メールポート 1（ml1）で指定された宛先に送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set keep-alive-time 09,17 0      ← キープアライブ送信時刻の指定
[rmc@myrmc]# set spy rmc ml1                  ← ｷｰﾌﾟｱﾗｲﾌﾞ送信先ﾒｰﾙﾎﾟｰﾄの指定
[rmc@myrmc]# set mail-service                 ← メールサービスの開始
[rmc@myrmc]# disable
rmc@myrmc >
```

## 6.5　SNMP エージェントの機能と設定

RMC Version2.1 以上では、新たに SNMP エージェント機能が搭載されています。この機能を利用することにより、RM-CM 自身を SNMP マネージャから監視することが可能になります。

### SNMP エージェント機能の設定

SNMP エージェント機能を利用する場合は、**set snmp-community** コマンドにより SNMP エージェントを起動し、コミュニティ名の設定およびネットワークのアクセス許可の設定を行います。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set snmp-community xxxxxxx    ← エージェントの起動、コミュニティ名の設定
[rmc@myrmc]# disable
rmc@myrmc >
```

### SNMP Trap の設定

SNMP Trap 機能により、トラップ情報の送信を行うことも可能です。送信されるトラップ情報は、"ColdStart Trap" 及び "WarmStart Trap" です。この機能を有効にした場合、RM-CM のブート時にトラップ情報が指定のホストに送出されます。

この利用する場合は、**set snmp-traps** コマンドでトラップ送信先の IP アドレスもしくはホ

スト名、およびコミュニティ名を設定します。

```
rmc@myrmc > enable
password：
[rmc@myrmc]# set snmp-traps xxx.xxx.xxx.xxx yyyyyyy
                                                    ← 送信先ホスト名、コミュニティ名の設定
[rmc@myrmc]# write memory                          ← 設定情報をファイルに保存
[rmc@myrmc]# disable
rmc@myrmc >
```

**set snmp-traps** で指定されるコミュニティ名は、**set snmp-community** で指定されるコミュニティ名との関連はありません。

"ColdStart Trap" を発信させる為に、上記設定後は、必ず **write memory** を実行して設定情報を設定ファイルに保存してください。

# 7. RMS(RouteMagic Server)利用時の設定

RMS を利用する場合は、RM-CM－RMS 間の通信仕様に合わせた設定が必要になります。本章の記述に従って、各ポート、およびセキュリティ関連の設定を行ってください。

RM-CM と通信する RMS は、Version3.0 以上が必要です。

## 7.1 メールポート(ml0)と COM ポート(comN)の設定

RM-CM はメールポート 0 (ml0) を使用して RMS と通信を行います。以下に、COM1 に監視対象装置として Cisco 社製品を接続する場合の設定例を示します。Cisco 製品以外の装置を監視対象として RMS を利用する場合は、後述の一般機器接続に必要な設定事項に関する記載を参照して、事前に装置種別とフィルタ・スクリプトのユーザ定義を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port ml0                        ← カレントポートを ml0 に指定
[rmc@myrmc(ml0)]# set mailto RMS@routrek.co.jp   ← RMS のメールアドレスを設定
        COM ポートごとに接続する装置の台数分設定
[rmc@myrmc(ml0)]# set spy com1 tfl0 ml0          ← com1 をメールポート 0 に接続
[rmc@myrmc(ml0)]# set port com1                  ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set target-type cisco         ← com1 の装置種別を cisco に指定
[rmc@myrmc(com1)]# set target-login-password passwd1
                                       ← 監視対象装置のﾊﾟｽﾜｰﾄﾞを設定
[rmc@myrmc(com1)]# set target-enable-password passwd2
                                       ← 監視対象装置の特権ﾓｰﾄﾞﾊﾟｽﾜｰﾄﾞを設定
[rmc@myrmc(com1)]# set target-check              ← 監視対象装置の生存確認を行う
[rmc@myrmc(com1)]# set network-info-time h m     ← h 時 m 分にﾈｯﾄﾜｰｸ情報を送信
[rmc@myrmc(com1)]# set connect-log               ← connect ログを記録する
[rmc@myrmc(com1)]# set spy target1 ml0           ← 生存確認･ﾈｯﾄﾜｰｸ情報･操作ログ
                                                   の送信先メールポートを設定
[rmc@myrmc(com1)]# set spy rmc ml0               ← ｷｰﾌﾟｱﾗｲﾌﾞ情報の送信先を設定
[rmc@myrmc(com1)]# show running-config           ← RM-CM の設定を確認
[rmc@myrmc(com1)]# set mail-service              ← メールサービスの開始
[rmc@myrmc(ml0)]# disable
rmc@myrmc >
```

上記の RMS メールアドレスは参考例です。各システムに適したアドレスを設定してください。

RMS のプラグイン機能をご利用の場合は、➡「RMS プラグイン ユーザーズガイド」を参照して、必要な設定を行ってください。

# 7.2　セキュリティ関連の設定

## メールの暗号化と認証に関する設定

暗号化には、PGP(GnuPG)を使用する方法とルートレック独自の暗号化方式（RES: Routrek Encryption Scheme）を使用する方法の 2 種類があります。

Internet 経由で RMS と通信する場合は、セキュリティ保持のため必ずメールの暗号化と認証の設定を行ってください。

> 工場出荷時は **set mail-certification**（受信メールの認証）が指定された状態となっています。暗号化と認証が不要な場合は、**set no mail-certification** を実行してメールの認証指定を解除してください。

### ■ PGP を使用する場合

PGP を使用する場合、送信メールの暗号化と受信メールの認証が行われます。設定には、RMS のメールアドレスをキーID とした PGP 公開鍵が必要です。PGP 公開鍵は、RMS の管理者により発行されます。

```
set public-key              ← RMS の PGP 公開鍵を設定
show key-list               ← 登録された PGP 公開鍵を確認
set port ml0
set mail-encryption         ← 送信メール内容の暗号化を行う
set mail-certification      ← RMS からの受信メールに対する認証を行う
```

### ■ RES（独自暗号化方式）を使用する場合

RES を使用する場合、送受信メールの両方が暗号化されます。暗号化に必要な鍵は RMS と RM-CM がお互いにメールを送受信することで自動的に設定されます。

```
set port ml0
set mail-encryption res     ← RMS に送信するメールを RES 暗号化する
set mail-certification      ← RMS から RES 暗号化メールを受信する
```

RES には、従来の PGP に比べて以下のようなメリット･デメリットがあります。

| メリット | デメリット |
|---|---|
| 鍵の設定が不要で､セットアップの手間が軽減できる | RMS と RM-CM の間でメールの送受信両方が可能でないと利用できない |
| 送信メールだけでなく､受信メールも暗号化できる | PGP に比べ、なりすまし問題(Man in the middle attack)に弱い |

**RMS 用 SSH パスワードの設定**

RMS から RM-CM にコマンドを発行する際、通常はメールが利用されますが、RMS から RM-CM に直接 SSH ログインが可能な環境の場合は、SSH 経由でのコマンド発行も可能です。

RM-CM と RMS 間のメール送受信に RES（独自暗号化方式）が使用されている場合、SSH ログイン用パスワードは自動で設定されます。そうでない場合は、RMS と RM-CM の両方に共通の SSH ログイン用パスワードを設定する必要があります。RM-CM 側の設定は、以下に例を示すように、ユーザ ID "rms" に対して SSH パスワードを設定してください。

**set user-password rms foo**　　← ユーザ ID "rms" にパスワード "foo" を設定

SSH を使用する場合は、RMS 側にもコマンド発行時に SSH を使用するための設定が必要です。設定に関しては、RMS の管理者にご確認ください。
➡「RMS ユーザーズガイド　～オーナ管理者編～　4.1 RM-CM 設定情報の登録と参照」参照

## *7.3　フィルタの設定*

監視対象装置が Cisco 製品(ルータ、スイッチ)の場合、メールポート 0 (ml0) には、デフォルトフィルタ 0 (tfl0)が設定されている必要があります。RMS との通信を開始する前に以下のコマンドを実行して工場出荷時の状態に戻してください。

**set spy *comN* tfl0 ml0**

監視対象装置が Cisco 製品以外の場合は、装置から出力されるメッセージの形式に合わせたフィルタの設定を行ってください。　➡「15. ユーザ定義フィルタの作成」参照

## *7.4　RMS への RM-CM の登録*

RMS は、RM-CM から送信される "Setup information" メールの受信によって RM-CM を識別し、RMS 上での管理を可能にします。

"Setup information" メールは、RM-CM の起動時および設定変更時に自動的に送信されますが、手動送信することも可能です。RMS の初期設定などの都合により強制的に "Setup information" を送信したい場合は、下記のコマンドを実行してください。

**mail-test setupinfo ml0**

# 8. セキュリティに配慮した運用

セキュリティを重視することが必要な環境に RM-CM を設置する場合は、以下のような設定を行ってください。

## 8.1 ユーザ名、パスワードの設定

### パスワードの管理

RM-CM のログインパスワードや特権パスワードを適切に設定・管理することが重要です。
設定は、**set password,　set enable-password** コマンドで行います。

➡「3.3　パスワードの設定」参照

### ユーザ名の管理

RM-CM にログインする際のユーザ名は、初期状態では "rmc" が設定されています。各 RM-CM に別の名称を設定することにより、不正ログインに対するセキュリティを向上させてください。

ユーザ名の登録は、**set use-rname** コマンドを実行し、ユーザ名とパスワードを設定することにより行います。

ユーザ名の追加後、デフォルトのユーザ名“rmc”を無効にしてください。ただし、デフォルト・ユーザ名“rmc”は、通常の削除コマンド（set no user-name）では削除することができません。
**set user-name2 rmc＊** コマンドを実行することにより、無効にしてください。

➡「3.5　ログインユーザの追加」参照

## 8.2 ssh(Secure SHell) の使用

ネットワーク経由で RM-CM にログインする場合、telnet ではなく ssh のご利用をおすすめします。RM-CM とターミナル間の通信が暗号化されるため、ネットワークの盗聴などに対するセキュリティが向上します。

また、ssh を使用する際は、telnet ログインを無効にしておくことをおすすめします。
設定は **set access-list deny telnet 0.0.0.0** コマンドによって行います。

## 8.3 RM-CM に対するアクセス制限の設定

RM-CM では telnet, ssh, smtp(メール受信), snmp, tftp, connect-port(端末からール com ポートへ直接 telnet 接続)の各プロトコルについて、特定の相手に限り接続を許可・不許可にすることができます。

> 初期設定ではすべて許可になっているので、外部のネットワークに接続する場合は、必ずアクセス制限を設定してください。

アクセス制限を行う場合、許可するアドレスを **set access-list allow {*プロトコル名*} {*IP アドレス*}** コマンドで登録後、それ以外のアドレスからの接続はすべて不許可（ **set access-list allow {*プロトコル名*} 0.0.0.0**）にすることをおすすめします。

例として、192.168.0.* からの ssh ログインだけを許可する場合、以下のコマンドを実行します。

```
set access-list allow ssh 192.168.0.0/24
set access-list deny ssh 0.0.0.0
```

また、全てのプロトコルに対して一括してアクセス制限を行う場合、以下の例のようにプロトコルに **all** を指定してください。

```
set access-list deny all 0.0.0.0
```

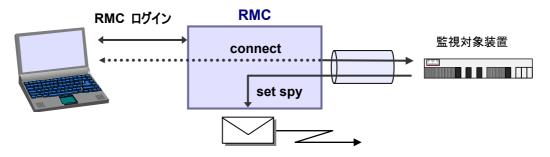
## 8.4 送信メールの暗号化

RM-CM には PGP を使用して送信メールの暗号化と、受信メールの認証を行う機能があります。メールを暗号化するには、メールアドレスをキーとした PGP 公開鍵を別途用意し、それを **set public-key** コマンドで RM-CM に設定する必要があります。その後、暗号化メールを送信するメールポートに対して **set mail-encryption** を実行すると、送信されるメールが暗号化されます。

なお、暗号化の有無はメールポート毎に設定できます。また、RM-CM から送信した暗号化メールを受け取るには、電子メールソフト(MUA)の側も PGP 暗号化メールに対応している必要があります。

# 9. 監視対象装置の操作とログの表示

## 9.1　監視対象装置との接続

COM ポートに接続された監視対象装置は、RM-CM にログインしている端末から直接操作することができます。監視対象装置にログインする場合は、RM-CM にログインした後、現在の標準入出力と *comN* ポートを **connect** コマンドにより双方向接続します。connect コマンド実行後、RM-CM は監視対象装置のシリアルコンソールとして動作します。

connect 実行中の操作記録は、**set spy** コマンドで *targetN* ポート（*comN* に対応する仮想ポート）に接続されたメールポートから送信されます。デフォルトのメールポートとしては、ml0 が設定されています。

**connect ログの送信**

connect 実行中の操作と装置からの出力は com*N* ポートに対しては行われず、target*N* ポートだけに入力されます。*targetN* ポートへの入力は Target operation log(*comN*)として、set spy コマンドで各ポートに接続されたメールポートから送信されます。connect 中の装置出力は、*comN* ポートに対して入力されないため、不要な操作ログが Target message(*comN*)としてメール送信されることはありません。

## 9.2　connect 時の操作

① RM-CM にログインします。

② 特権モード（**enable** コマンド実行）に移行した後、操作する監視対象装置が接続されている COM ポートを指定して、**connect** コマンドを実行します。

③ 監視対象装置の操作を行います。（装置のコンソールとして操作できます）

④ connect を終了します。
connect は、エスケープキャラクタ(Ctrl－¥)に続けて x を入力するか、他の端末から **disconnect** コマンドを実行することにより終了します。

*targetN* ポートからの connect ログは、connect の開始から終了までの単位で送信されます。終了操作を実行するまで、connect ログは送信されませんのでご注意ください。RM-CM 自身との接続を終了した場合（Ex. telnet 接続の切断時）も、connect は自動的に終了します。

以下に、COM1 に接続された Cisco 装置に対する **connect** の実行例を示します。
内は、監視対象装置に対する操作内容を示しています。

```
myrmc login: rmc                              ← RMC へのログイン
Password:
[rmc@myrmc]# connect com1                     ← 標準入出力を com1 に接続
Escape character is CTRL-¥
Press 'CTRL-¥ x' to disconnect.

2924XL>show version
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:34 by devgoyal
Image text-base: 0x00003000, data-base: 0x003331F4
                    ・
                    ・
                  (省略)
2924XL>ok                                     ← Ctrl - ¥ に続き x を入力
[rmc@myrmc]#                                    (標準入出力との接続を終了)
```

## 9.3　監視対象装置との直接接続

端末から RM-CM の特定ポート番号に telnet 接続することで、端末と COM ポートを直接接続することが可能です。

本機能を有効にするには、あらかじめ **set connect-port** コマンドの指定が必要です。以下に、直接接続のための telnet ポートを 7001 番に指定する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set connect-port 7001            ← 直接接続のための telnet ポートを指定
[rmc@myrmc]# show log mail 20                 ← メール送信ログを 20 行表示
[rmc@myrmc]# disable
rmc@myrmc >
```

上記の例の場合、telnet ポート番号と COM ポートとの対応は以下のようになります。

7001 番ポートに telnet　:　COM1 に接続

7002 番ポートに telnet　:　COM2 に接続

## 9.4 透過モードでの接続

XMODEM ファイル転送など、端末 - 監視対象装置 間でバイナリデータが送受信される場合は、接続モードを透過モードにする必要があります。透過モードでは BREAK 信号を除く全てのデータが、そのまま端末 - 監視対象装置間で送受信されます。

- **透過モードへの移行**：

  接続実行中にエスケープキャラクタ(Ctrl-¥)に続けて t を入力します。
  これ以降は透過モードとなり、エスケープキャラクタの入力も不可になります。

- **透過モードの終了**：

  シリアルまたは telnet で RM-CM にログインしている場合は、端末から RM-CM に対して BREAK 信号を送信してください。
  ssh で RM-CM にログインしている場合は、透過モード終了の手段はありません。端末側で ssh 接続を強制切断するか、別の端末から disconnect コマンドを実行してください。

## 9.5 直接接続時の操作

① 端末から RM-CM の指定したポートに対して telnet 接続します。
② 通常のログイン操作の後、監視対象装置に直接接続されます。
③ 監視対象装置の操作を行います。(装置のコンソールとして操作できます)
④ 直接接続を終了します。

connect コマンド実行時と同様に、エスケープキャラクタ(Ctrl-¥)に続けて x を入力するか、他の端末から disconnect コマンドを実行することにより終了します。なお、終了後は telnet 接続も切断されます。

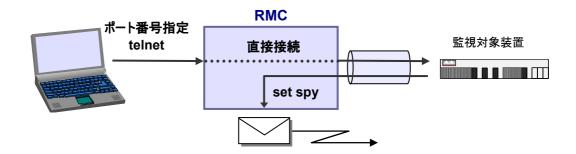
以下に、COM1 に接続された装置に対する直接接続の実行例を示します。なお、本操作に先立ち、set connect-port 7001 が実行されているものとします。

```
<RMC の 7002 番ポートに telnet ログイン>
myrmc login: rmc1                              ← rmc1 ユーザが RMC にログイン
Password:
RouteMagic Console Manager. RM-CM200 Version 3.0.0ED6
Copyright (C) 2003 Routrek Networks, Inc. All Rights Reserved.
Connecting to com1                             ← 接続 COM ポートの表示
Escape character is CTRL-¥
Press 'CTRL-¥ x' to disconnect                 ← 以降、connect コマンド実行時と同様
```

# 9.6 接続時の注意

## 複数ユーザからの接続要求

１つの COM ポートに対する接続は、複数ユーザから同時に実行することはできません。上記の例に示した接続実行中に、他のユーザが同一の COM ポートに接続を要求した場合、下記のようなエラーメッセージが表示され、接続は実行されません。
この場合、特権ユーザは、disconnect コマンドを使用して他のユーザの接続を強制切断することが可能です。

```
myrmc login: rmc1                          ← rmc1 ユーザが RMC にログイン
Password:
[rmc1@ myrmc]# connect com1                ← com1 に対する connect を実行
Locked by user rmc                         ← "rmc"ユーザが connect 中であることを
error!                                        示すエラーメッセージ
[rmc1@myrmc]# disconnect com2              ← 他ユーザの接続を強制切断
```

## RM-CM による装置の操作

接続中の装置に対しては、RM-CM から自動ログインして操作を行うことができません。このため、接続状態を長時間継続すると、"Network-info" による装置情報の定期送信や RMS からのコマンド発行などでエラーが発生する可能性がありますので、ご注意ください。

このような状況が発生した場合、RM-CM はサブジェクト"Target command error(*comN*)" のメールを送信してエラーの発生を通知します。例えば、Network-info 送信の実行時にエラーが発生した場合は、以下のような内容が通知されます。

---

Timed out for exclusive access to the target device.(Network Info)
Locked by user rmc

---

# 9.7　エスケープキャラクタの機能

接続中は、エスケープキャラクタに続けて以下の文字を入力することにより、エスケープコマンドとして使用することができます。エスケープキャラクタのデフォルトは、Ctrl－¥（Ctrl キーを押しながら¥キーを押す）に設定されています。

| 入力文字 | 入力後の動作 |
|---|---|
| x | disconnect（機器との接続を終了し、RM-CM シェルに戻る） |
| b | ブレーク信号を出力する |
| ? | エスケープコマンド入力時の動作を表示 |
| t | 透過モードへの移行 |
| Ctrl－¥ | エスケープキャラクタ自身を 1 文字出力 |
| その他の文字 | 入力された文字をそのまま出力 |

## エスケープキャラクタの変更

エスケープキャラクタは、任意のコントロールキャラクタ（Ctrl キーを押しながら入力される 1 文字)、またはエスケープキー（Esc）により入力される 1 文字に変更可能です。エスケープキャラクタの変更は **set escape-character** コマンドによって行い、引数に CTRL-？ または CONTROL-？（? は任意の 1 文字）もしくは ESC を指定します。

設定例：

| | |
|---|---|
| set escape-character CTRL－x | エスケープキャラクタを Ctrl－x に設定 |
| set escape-character ESC | エスケープキャラクタを Escape に設定 |

# 9.8　接続ユーザの制限

RM-CM では COM ポートごとに接続可能なユーザを指定する **set connect-users** コマンドが用意されています。以下に、COM1 ポートに接続できるユーザを operator1, operator2 に限定し、COM2 ポートには全てのユーザが接続できる設定を行う例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1
[rmc@myrmc(com1)]# set connect-users operator1 operator2 ← 接続可能ユーザを指定
[rmc@myrmc(com1)]# set port com2
[rmc@myrmc(com2)]# set no connect-users      ←接続可能ユーザの指定を解除
                                              （全ユーザが接続可能）
[rmc@myrmc(com2)]#
```

# 10. シリアルポートのログと装置設定情報の表示・保存

## 10.1 シリアルポートのログ表示

RM-CM では各シリアルポートから入力されたデータ(装置が出力した内容)のログを内部メモリに 300KB(RM-CM1200 は 600KB)分、格納しています。

ログの表示は、**show log *comN*** コマンドで行います。

ログの内容が 1 画面に収まらない場合、ページャが起動されます。

➡「4.2　ページャの操作」参照

なお、ログの表示を、**show log –t *comN*** と"-t"オプション付きで行った場合、各行の先頭にログの出力時刻を追加して表示します。

```
[rmc@ myrmc]# show log –t com1                    ← com1 のログを時刻付きで表示
2005/02/15 14:20:17|C2900XL POST: System Board Test: Passed
2005/02/15 14:20:17|C2900XL POST: Daughter Card Test: Passed
2005/02/15 14:20:17|C2900XL POST: CPU Buffer Test: Passed
2005/02/15 14:20:17|C2900XL POST: CPU Notify RAM Test: Passed
2005/02/15 14:20:18|C2900XL POST: CPU Interface Test: Passed
2005/02/15 14:20:18|C2900XL POST: Testing Switch Core: Passed
2005/02/15 14:20:18|C2900XL POST: Testing Buffer Table: Passed
2005/02/15 14:20:18|C2900XL POST: Data Buffer Test: Passed
2005/02/15 14:20:19|C2900XL POST: Configuring Switch Parameters: Passed
2005/02/15 14:20:22|C2900XL POST: Ethernet Controller Test: Passed
2005/02/15 14:20:30|C2900XL POST: MII Test: Passed
```

## 10.2 装置設定情報の表示

RM-CM では装置から定期的に収集した設定情報等を内部メモリに最大 512KB 分、格納しています。

情報収集のための設定に関しては、「6.3　監視対象装置とネットワーク関連情報の自動送信」をご参照ください。

装置設定情報の表示は、**show target-config comN** コマンドで行います。

ログの内容が 1 画面に収まらない場合、ページャが起動されます。

➡「4.2　ページャの操作」参照

## 10.3　シリアルポートのログおよび装置設定情報の保存

シリアルポートのログ、および装置の設定情報は、以下のタイミングで RM-CM 内部の不揮発性メモリに保存されます(保存サイズはログの場合各ポートあたり 300KB、装置設定情報は各ポートあたり最大 512KB)。

保存された内容は次回のRM-CM起動時に自動的に内部メモリに展開され、**show log comN**, **show target-config comN** コマンドで表示されます。

set network-info-time コマンドで設定された装置関連情報取得実行時
write log コマンド実行時
reload　※
shutdown コマンド実行時　※
※保存したくない場合は、"reload -f"のように"-f"オプションをつけてコマンド実行してください。

なお、ログおよび装置の設定情報は、以下のタイミングで消去されます。
clear log comN コマンド実行時
upgrade コマンド実行時

# 11. 監視対象装置の電源管理

電源管理製品と RM-CM とを連携して使用することで、監視対象装置の装置の電源を管理することが可能です。
たとえば、ソフトウェアリブートでは復旧しない障害の場合でも、電源のオン・オフによるハードウェアリセットを行うことが出来ます。

## 11.1 電源管理関連の設定

以下に COM1 に監視対象装置を、COM2 に RPM を接続し、監視対象装置の電源を明京電機株式会社製の LAN・デ・ブート・ミニ(RPC-4L)の 1 番コンセントに接続した場合の設定内容を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2                ← カレントポートを com2 に変更
[rmc@myrmc(com2)]# set target-type rpc    ← COM2 の装置種別として RPC を指定
[rmc@myrmc]# set port com1                ← カレントポートを com1 に変更
[rmc@myrmc(com1)]# set pmport com2 1      ← 電源が COM2 の RPM の 1 番
                                            コンセントに接続されていることを指定
```

## 11.2　装置の電源の操作

装置の電源は、target-power {comN} {on|off|reboot|status} コマンドで操作します。

引数には装置が接続されている COM ポートと、操作内容(on,off,再起動,ステータス表示)を指定します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2                ← カレントポートを com2 に変更
[rmc@myrmc(com2)]# set target-type rpc    ← COM2 の装置種別として RPC を指定
[rmc@myrmc]# set port com1                ← カレントポートを com1 に変更
[rmc@myrmc(com1)]# set pmport com2 1      ← 電源が COM2 の RPM の 1 番
                                            コンセントに接続されていることを指定
```

## 11.3　監視対象装置が無応答の場合の自動リブート設定

監視対象装置の生存確認の結果無応答であった場合、監視対象装置を自動でリブートまたは電源断を行う事が出来ます。

この機能を利用するには「11.1 電源管理関連の設定」を予め行っておく必要があります。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2                 ← カレントポートを com2 に変更
[rmc@myrmc(com2)]# set target-type rpc     ← COM2 の装置種別として RPC を指定
[rmc@myrmc]# set port com1                 ← カレントポートを com1 に変更
[rmc@myrmc(com1)]# set pmport com2 1       ← 電源が COM2 の RPM の 1 番
                                             コンセントに接続されていることを指定
[rmc@myrmc(com1)]# set target-check off    ← 生存確認の結果無応答であった場合
                                             監視対象装置の電源断を行う事を指定
```

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2
[rmc@myrmc(com2)]# set target-type rpc
[rmc@myrmc]# set port com1
[rmc@myrmc(com1)]# set pmport com2 1
[rmc@myrmc(com1)]# set target-check reboot 180 ←生存確認の結果無応答であった場合
                                             監視対象装置の再起動を行う事を指定
                                             （再起動までの待ち時間を 180 秒に設定）
```

# 12. 認証サーバ(RADIUS)対応

認証サーバを利用すれば、個々の RM-CM 毎にユーザ情報を管理するのではなく、ユーザ情報の一括管理が可能になります。RM-CM ではログイン認証に RADIUS 認証を利用することが出来ます。

## 12.1 認証方式の設定

認証方式の設定は、**set aaa-authentication** コマンドで行います。RM-CM 内部のユーザ情報でログイン認証を行う場合(デフォルト)は、**set aaa-authentication login local** コマンドを、RADIUS サーバを利用してログイン認証を行う場合は、**set aaa-authentication login radius** コマンドを実行します。

RM-CM ではログイン認証のみ RADIUS に対応しています。enable コマンドの実行に必要な特権パスワード、WEB インターフェース接続時の認証及び RM-CM の PPP サーバアカウントは RADIUS 認証に対応していません。

なお、RADIUS 認証を設定している場合、原則として RM-CM 内部のユーザ情報はログイン認証対象になりません。ただし、例外として RADIUS サーバが無応答の場合は、RM-CM 内部のユーザ情報でログイン認証を行います。

## 12.2 RADIUS サーバの設定

RADIUS サーバの設定は、**set radius-server** コマンドで行います。引数としてプライマリ/セカンダリサーバーの指定、サーバ名(+ポート番号)、および RADIUS サーバとの通信に必要な共有鍵を指定します。

以下に、設定例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set aaa-authentication login radius  ←ログイン認証方式に RADIUS を指定
[rmc@myrmc]# set radius-server 192.168.10.2 testing123
                                        ←RADIUS サーバの IP アドレス、共有鍵を指定
```

RADIUS 認証のテストを行う場合、もし認証が失敗した場合に備えて、必ず 1 つはログイン済みの端末を開いた状態で行うことをおすすめします。

# 13. その他の機能の利用と使用上の注意

## 13.1　RM-CM の設定の表示と保存

RM-CM は、下図に示すように 3 種類の設定情報を管理しています。各種のコマンドを実行して RM-CM に設定した内容は、"現在の設定"（running-config）に書き込まれます。この内容を保存せずに RM-CM を再起動(reload)した場合、最後に保存した設定(startup-config)を使用して RM-CM が起動され､現在の設定は破棄されます｡設定変更の作業を行った後は、必ず保存操作を行うようにしてください。

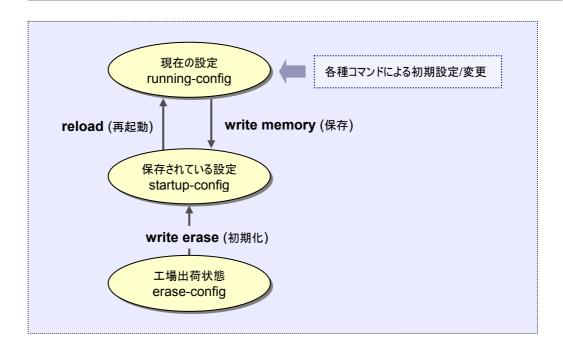
これらの設定情報の参照と保存は、以下のコマンドを使用して行います。

### 設定の表示

- **show running-config**　：現在の設定内容（running-config）を表示します。
- **show configuration**　：保存されている設定内容（startup-config）を表示します。
- **show port <ポート名>**　：各ポートごとの設定とステータスを表示します。
- **copy {running-config | startup-config} terminal**　：
  PGP キーやフィルタ・スクリプトの設定も含め、現在の設定もしくは保存されている設定の全項目を表示します。

### 設定の保存と保存内容の初期化

- **write memory**　：現在の設定内容を保存します。
- **write erase**　："保存されている設定"を初期化し、工場出荷状態に戻します。 "現在の設定" は、reload コマンドが実行されるまで変更されません。

> reload 実行時に、保存されていない設定変更項目が存在した場合、警告メッセージと共に未保存の設定項目が表示されます。

### 設定のバックアップとリストア

- **コンソール経由の場合**：

 ① バックアップ： **copy running-config terminal** を実行。

  現在の設定内容をすべて表示した後、表示内容を任意のファイルに保存します。

 ② 再設定： **write-erase** および **reload** 実行後、**copy terminal running-config** を実行。

  保存内容をコンソールにコピーすることにより、再設定を行うことができます。

  設定を保存する場合は write memory を実行してください。

- **コンソール経由の場合(XMODEM を利用)**：

 ① バックアップ： **copy running-config xmodem:** を実行。

  実行後、端末側で XMODEM ファイル受信を起動し、設定ファイルを保存します。

  ※XMODEM ファイル送受信を CRC チェック付きで行う場合は、"～ xmodem -c" のように"-c"オプションを付加してください。

 ② 再設定：**write erase** および **reload** 実行後、**copy xmodem running-config** を実行。

  実行後、端末側で XMODEM ファイル送信を起動し、保存されている設定ファイルを RM-CM に送信してください。

  設定を保存する場合は write memory を実行してください。

- **tftp 経由の場合**：

 ① バックアップ： **copy runnning-config tftp** を実行。

  現在の設定内容のすべてを tftp サーバに保存します。

 ② 再設定： **copy tftp startup-config** を実行後、**reload** を実行。

  tftp サーバに保存されたファイルによって”保存されている設定”を再設定した後、再起動により”現在の設定”を保存されていた状態に戻します。

## *13.2 RM-CM の電源のオフとハードウェアリセット*

RM-CM は以下に記述する動作中を除き、シャットダウン操作を実行せずに電源オフ、もしくはハードウェアリセット（RM-CM200 のみサポート）を行っても問題がないように作られていますが、電源をオフにする際は、**shutdown** コマンドを実行するようにしてください。

> **RM-CM1200** をご利用の場合、shutdown を実行せずに電源をオフするには、背面の電源スイッチを 4 秒間以上押し続ける必要があります。

### 電源オフを行ってはならない RM-CM 動作状態

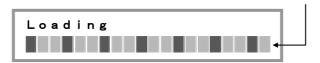
- **システムのブート時**　（RM-CM1200：LCD に Loading が表示されている間）<br>（RM-CM200 ：ステータス LED が回転表示の間）

- **システムのシャットダウン時（再起動を含む）**

- 以下のコマンド実行中

| | |
|---|---|
| **write memory** | 設定情報の保存用コマンド |
| **write erase** | 設定情報の削除コマンド |
| **write log** | シリアルポートのログ保存コマンド |
| **clear log** | シリアルポートのログ消去コマンド |
| **copy** | 設定情報の保存・復帰用コマンド |
| **upgrade** | RM-CM ソフトウェアのアップグレードコマンド |
| **target-test** | 装置の生存確認および装置情報の取得テスト |

上記動作の実行中、LCD およびステータス LED の表示は以下のようになります。

**RM-CM1200**：LCD の下段が下図のような ”アニメーション表示” になります。

**RM-CM200** ：ステータス LED が回転表示になります。

- ファンクションスイッチで 機能番号"9"または"A" を実行中（**RM-CM200 のみ**）

➡「13.4　ファンクションスイッチの使用方法（RM-CM200）」参照

## *13.3　LCD 操作パネルの使用方法（RM-CM1200）*

RM-CM1200 では、前面に配置された LCD 表示パネルと矢印ボタン、A/B ボタンを利用することによって、各種のステータス確認を簡単に行うことができます。

### ■ LCD 表示パネル

20 文字ずつ上下 2 段表示で、IP アドレスを始めとする各種ステータス、操作パネルから実行するメニューの表示などが行われます。

### ■ 矢印ボタンの機能

| | |
|---|---|
| 上下ボタン | ：メニューの選択、およびメニューモードでの項目選択などに使用します。 |
| 左右ボタン | ：左右のスクロール、カーソルの移動に使用します。 |

### ■ A/B ボタンの機能

| | | |
|---|---|---|
| A | A ボタン | ：表示中の機能を実行します。 |
| B | B ボタン | ：操作をキャンセルします。 |

## 通常モードの表示と機能

通常、LCD 表示パネルには下図のように上段にイーサネットポート名と IP アドレス、下段に banner 文字列（もしくは "RM-CM1200"）が表示されています。banner 文字列は、**set banner** コマンドで任意に設定可能です。

```
ＥＴＨ０：１９２．１６８．１０．１８５
RM-CM１２００
```

この状態では、次の操作が可能です。

- **イーサネットポートの指定**

  A/B ボタン によって、選択したイーサネットポートのアドレスを表示します。

  LCD 上段の表示は、A/B ボタンを押すと "ETH0 アドレス"、"ETH1 アドレス"、"Press UP／DN for menu" に変化します。

- **操作メニューの表示**

  上下ボタン を押すと、LCD に操作メニューが表示されメニューモードになります。

- **スクロール**

  左右ボタン を押すことにより、LCD 下段の banner 文字列がスクロールします。

## メニューモードの表示と機能

通常モードで上下ボタンを押すとメニューモードとなり、図のように LCD 上段にメニューが表示されます。以下の操作でメニューの選択を行ってください。

```
０：　RM-CM　ｓｏｆｔ　ｖｅｒｓｉｏ
```

① 上下ボタン でメニューを選択します：

LCD 上段に選択中のメニューが表示されます。

② 実行すべきメニューが表示されたら、A ボタン を押します：

選択したメニューの実行が開始されます。

■ **LCD 操作メニュー**

LCD 操作パネルから実行可能な操作メニューには、次の種類があります。

| メニュー表示 | 機能 |
|---|---|
| 0：RM-CM soft version | RM-CM に搭載されているソフトウェアのバージョンおよび現在の時刻を表示 |
| 1：COM port status | COMA／B、COM1～COM12（シリアルポート）のステータスを表示 |
| 2：ETH port status | ETH0／1（イーサネットポート）のステータスを表示 |
| 3：Set ETH IP addr | ETH0／1（イーサネットポート）の IP アドレスを設定 |
| 4：Set ETH speed | ETH0／1（イーサネットポート）の通信速度と通信方式（10／100Mbps、全二重／半二重）を選択 |
| 5：Set LCD light | LCD バックライトの ON／OFF を指定 |
| 6：Write config | RM-CM 設定情報の保存を実行 |
| 7：Restart／Halt RM-CM | 再起動（Restart）／シャットダウン（Halt）を実行 |
| 8：Erase config | RM-CM の設定を初期化（工場出荷状態に戻す） |

メニュー番号 3、4 および 5 で設定した IP アドレス、イーサネット通信速度、LCD バックライトの指定を RM-CM の再起動後も有効とするには、設定情報の保存（メニュー6）を実行する必要があります。

■ **メニュー機能実行中のボタン操作**

各メニュー項目の実行開始後は、選択したメニューによって各ボタンの機能が異なります。LCD 表示において、各ボタンは次のように示されます。LCD に表示されるガイダンスに従ってメニューを実行してください。いずれのメニューにおいても、一定時間操作を行わないと通常モードの IP アドレス表示状態に戻ります。

| 上下ボタン | ＵＰ／ＤＯＷＮ |
|---|---|
| A/B ボタン | Ａ　または　Ｂ |

## 操作例 1 ： COM ポートステータスの表示

① 通常モードで 上下ボタン を押し、下記のメニューを表示。

```
１：　ＣＯＭ　ｐｏｒｔ　ｓｔａｔｕｓ
```

② Ａボタン により、表示するポートを選択。

```
ＣＯＭ１：　９６００　ＣＴＳ｜ＤＳＲ
＜Ｎｏ　ｄｅｓｃｒｉｐｔｉｏｎ＞
```

LCD 下段には、当該 COM ポートに設定された Description が表示されます。
Description は、**set description** コマンドで任意に設定可能です。

## 操作例 2 ： ERASE config の実行

① 通常モードで 上下ボタン を押し、下記のメニューを表示。

```
8：  ERASE  config
```

② Ａボタン を押すと、下記の確認メッセージが表示される。

```
ERASE  config  ？
OK：A  CANCEL：B
```

③ Ａボタン で実行開始、実行しない場合は Ｂボタン でキャンセル。

## 操作例 3 ： IP アドレスの設定

① 通常モードで 上下ボタン を押し、下記のメニューを表示。

```
3：  Set  ETH  IP  addr
```

② Ａボタン を押すとポート選択要求メッセージが表示される。

```
Select  ETH  port
A：ETH0  B：ETH1
```

③ Ａボタン または Ｂボタン を押し、アドレス設定対象のポートを選択。

④ 下記の内容が表示されたら、ボタン操作によりアドレスを設定。

```
Set  IP  address
000．000．000．000／00
```

カーソル位置

上下ボタン により設定値を指定（カーソル位置の数字が変化する）

左右ボタン によりカーソル位置を移動

⑤ 設定が完了したら、Ａボタン を押す。

```
192．168．000．001／24
OK：A   CANCEL：B
```

⑥　設定内容を確認し、 Aボタン を押す。

設定をキャンセルする場合は、 Bボタン を押す。

## 13.4　ファンクションスイッチの使用方法（RM-CM200）

RM-CM200では、製品正面の"FUNC"スイッチを使用して、特定の機能を実行させることができます。

ファンクションスイッチ

機能番号の選択

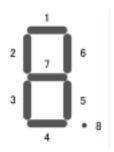
"FUNC"スイッチを押すとステータスLEDに"0."が表示され、機能番号の選択モードになります。ステータス LED の表示（機能番号）は、スイッチを押すたびにカウントアップされます。実行したい機能の番号が表示された時点でスイッチを1秒以上押し続けてください。表示が点滅した後に、指定した番号の機能が実行されます。

10秒以上スイッチを押さなかった場合は機能選択を中断し、通常のIPアドレス表示状態に戻ります。

ステータスLEDに表示される機能番号とRM-CMの動作は、次の通りです。

| 表示 | RM-CM 動作 |
|---|---|
| 0 | LEDにソフトウェアバージョン、及び日付と時刻を表示する |
| 1 | LEDにCOM1ポートの制御信号状態を表示する（下図参照） |
| 2 | LEDにCOM2ポートの制御信号状態を表示する（下図参照） |
| 3 | COM2ポートの設定をデフォルト値に戻し、ローカルコンソールに設定<br>（ログイン中の全ユーザは強制的にログアウトされます） |
| 4 | IPアドレスを自動設定する<br>（本機能実行の際は、あらかじめRM-CMをネットワークに接続してください） |
| 5-6 | shutdownコマンドを実行（システムを停止） |
| 7-8 | reloadコマンドを実行（シャットダウン後、システムを再起動） |
| 9 | write erase, reload コマンドを実行（設定値を工場出荷時の値に戻して、再起動） |
| A | write memory, reloadコマンドを実行（設定を保存して、再起動） |

制御信号状態の表示

制御信号は下図のようにステータス LED に表示され、制御信号が"オン"の状態で点灯します。状態表示を 4 秒間継続した後、COM ポートの通信速度が表示されます。

1: 未使用
2: RTS
3: CTS
4: 未使用
5: DTR
6: DSR
7: 未使用
8: COM1(on) / COM2(off)

## *13.5 telnet/ssh クライアント機能の利用*

RMC Version3.6 では、telnet/ssh クライアント機能をサポートしています。RM-CM を経由して、ネットワーク内の機器にログインすることができます。
telnet/ssh クライアント機能は標準では無効になっています。有効にするためには、**set options** コマンドを実行して、、telnet/ssh クライアント機能を有効にしてください。以下にに例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set options client=telnet          ← telnet クライアント機能を有効にする
[rmc@myrmc]# set options client=ssh             ← ssh クライアント機能を有効にする
[rmc@myrmc]# set options client=telnet,ssh      ← telnet,ssh クライアントの両方を有効に
                                                  する
[rmc@myrmc]# disable
rmc@myrmc >
```

■ telnet クライアント機能

RM-CM にログインした状態で、以下の例のように **telnet** コマンドを実行します。

```
rmc@myrmc> telnet 192.168.0.1
Entering character mode
Escape character is '^]'.
rmc@myrmc>
```

telnet ログイン先でログアウト処理を行うと接続は自動的に切断されますが、接続を強制切断する場合は、エスケープキャラクタ Ctrl-] に続けて e キーを押してください。

■ ssh クライアント機能

RM-CM にログインした状態で、以下の例のように **ssh** コマンドを実行します。

```
rmc@myrmc> ssh 192.168.10.1
Escape character is '~'. Hit '~.' to disconnect.
rmc@myrmc>
```

初めて接続する装置の場合、下記の例のようにホスト公開鍵の登録を行っていいかどうかの確認メッセージが表示されます。必要な場合は、ホスト公開鍵の正当性を確認した後、yes を入力してください。

---

The authenticity of host '192.168.10.1 (192.168.10.1)' can't be established.
DSA key fingerprint is b7:ae:3a:7f:c6:b3:fc:fb:af:80:19:6d:f6:b6:3d:8e.
Are you sure you want to continue connecting (yes/no)?

---

yes を入力すると、ホスト公開鍵は RM-CM に登録されますが、再起動後でもホスト公開鍵を有効にするには"write memory"コマンドを実行してください。設定とともにホスト公開鍵も保存されます。

なお、RM-CM にすでに登録済みのホスト公開鍵と、実際に取得したホスト公開鍵が異なる場合は、下記のエラーメッセージが表示され ssh 接続が失敗します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# ssh 192.168.0.1
Escape character is '~'. Hit '~.' to disconnect.


@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
a0:c4:31:4c:d8:9a:41:ab:2b:9e:0b:46:e4:66:4e:9c.
<中略>
Host key verification failed.
error!
[rmc@myrmc]#
```

RM-CM に登録されているホスト公開鍵を削除したい場合は、"-d"オプション付きで ssh コマンドを実行してください。RM-CM に登録されているホスト公開鍵をいったん削除した後に ssh 接続を行います。

ssh ログイン先でログアウト処理を行うと接続は自動的に切断されますが、接続を強制切断する場合は、エスケープキャラクタ ~ に続けて . キーを押してください。

## 13.6 リモートホストポートへの接続機能

RM-CM Version4.0 では、connect コマンドを使用してリモートホストへ telnet,ssh 接続することができます。connect コマンドによるリモートホストへの接続機能は、telnet/ssh クライアント機能とは違い、接続中の操作ログが記録されます。
記録された操作ログは show log rhpN コマンドで参照することが出来ます。。

```
rmc@myrmc > enable
password:
[rmc@myrmc(rhp1)]# set port rhp1          ← リモートホストポートをカレントに指定
[rmc@myrmc(rhp1)]# set remote-host 192.168.0.10  ← 接続先アドレスの指定
[rmc@myrmc(rhp1)]# set protocol telnet ← 接続のプロトコルを指定
[rmc@myrmc(rhp1)]# connect rhp1           ← 以降ログアウトするまでの操作ログが記録される
Vine Linux 2.1.5                           ←ログイン中
Kernel 2.2.18-0vl4.2 on an i686
login: testid
Password:
Last login: Thu Mar 1 10:00:10 from 192.168.0.9
[testid@host1 testid]$ logout             ←ここまでリモートホストへログイン中
[rmc@myrmc(rhp1)]# disable
rmc@myrmc >
```

# 14. 一般機器の接続とフィルタ・スクリプト

RM-CM にはコンソールポートを持つ各種の機器を接続して監視することが可能ですが、一般機器（Cisco 社のルータ／スイッチ以外の装置）を監視する場合は、各装置に適した設定が必要とされます。本章では、Cisco 製品以外の装置を監視対象とする場合の基本条件と一般機器の監視に必要なフィルタ・スクリプトの機能概要を説明します。

本章の記述内容は、RMC Version 2.1.0 またはそれ以上のソフトウェアに対応しています。Version 2.1.0 以前のソフトウェアでは、本仕様のフィルタ・スクリプトには対応しておりませんのでご注意ください。

## 14.1 システム組み込みのフィルタ・スクリプト

RMC Version3.5 からは、Cisco 以外の装置用フィルタ・スクリプトがあらかじめ用意されています。サポートされている装置種類は、**show version** で一覧が表示されます。これらの装置に関しては、後述の **set target-type** で装置種別の設定を行うだけで、利用が可能になります。その他の詳細に関しては、「RM-CM リリースノート」をご参照ください。

## 14.2 一般機器の接続要件

RM-CM に接続して監視対象とする装置は、以下の基本条件を満たす必要があります。

- **RS-232C/D 仕様のコンソールポートを持つこと**

  RM-CM との接続における必須要件です。

- **コンソールポートが ダム端末（ASCII 端末）接続可能な機能性を提供すること**

  RM-CM を経由した装置のリモート操作および､装置からの自動的な情報取得に必要な機能です。RM-CM の動作は、装置がコマンドライン・インタフェースを提供することを前提に定義されています。

- **エラーメッセージ、その他ログをコンソールポートに出力可能であること**

  コンソールポートからの出力情報によって装置の監視を行うために必要な機能です。原則として、この情報は RM-CM からの要求がなくとも、各装置の状態に従って自動的に出力されることを前提としています。

## 14.3 一般機器接続時の設定とフィルタ・スクリプトの機能

監視対象装置を接続する COM ポートには、接続する装置の種類（装置種別）を設定する必要があります。工場出荷時には、デフォルトの装置種別“**cisco**”が設定され、RM-CM はこの「装置種別」に対応するフィルタとスクリプトを使用して各種の機能を提供します。

一般機器（Cisco ルータ／スイッチ以外の装置）を接続する場合は、以下の設定が必要です。

■ **ユーザ定義の装置種別の宣言 ： set user-target-type {*装置種別名*}**

接続する装置の種類ごとに **set user-target-type** コマンドで装置種別をユーザ定義します。（Cisco 製品を接続してフィルタを追加定義する場合には、装置種別のユーザ定義は不要です。）

■ **COM ポートに対する装置種別の設定 ： set target-type {*装置種別名*}**

ユーザ定義した種別の装置を接続する COM ポートに対して、**set target-type** コマンドで装置種別の設定を行います。

■ **フィルタの作成 ： set target-filter {*装置種別名*} {*tflN* | config}**

デフォルトフィルタ以外のメッセージ抽出方法を定義する場合は、**set target-filter** コマンドにより、ユーザ定義のフィルタを作成します。（装置種別 **"cisco"** に設定されているデフォルトフィルタに関しては、➡「6.1 フィルタ機能の利用とデフォルトフィルタ」参照）

■ **スクリプトの作成 ： set target-script {*装置種別名*} {*スクリプトの種類*}**

監視対象装置の生存確認（set target-check）、装置情報の自動送信（set network-info-time）、RMS からのコマンド実行要求処理は、以下の 4 種類のスクリプトを使用して実行されます。スクリプトの設定は **set target-script** コマンドによって行い、各々の機能を実行するために必要な監視対象装置に対する操作や発行すべきコマンドを定義します。

| スクリプトの種類 | 機能 |
|---|---|
| target-check | 監視対象装置の生存確認に必要な操作を実行 |
| network-info | 監視対象装置とネットワーク情報の自動送信時に発行するコマンドを定義 |
| command | 監視対象装置に対するコマンド発行の処理を実行<br>（発行されるコマンドは、network-info スクリプト、および RMS で定義） |
| login | 監視対象装置への自動ログイン操作を実行<br>（装置へのログインが必要な、他のスクリプト実行時に利用される） |

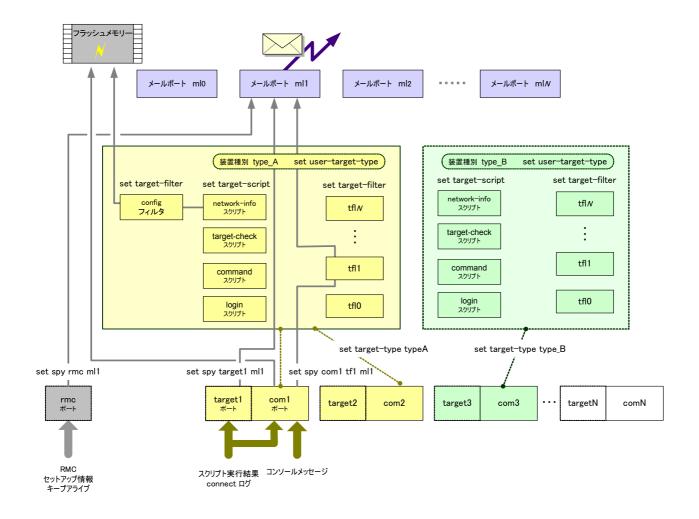
■ **スクリプト実行結果の送信**

上記スクリプトの実行結果は、***comN*** ポートおよび ***targetN*** ポートに接続されたメールポートから送信されます。送信先の指定は、**set spy *targetN mlN*** コマンドによって行います。コマンド発行結果などの情報が *comN* ポートから Target message(*comN*)としてメール送信されることを避けるには、*comN* ポートの set spy 設定時に適切なフィルタを指定してください。

### 関連コマンドリスト

| 全ての装置に共通の設定項目 | |
|---|---|
| 監視対象装置からの出力メッセージに適用するフィルタと送信メールポート | set spy *comN tflN mlN* |
| RM-CM 生存確認（keep-alive）の送信メールポート | set spy *rmc mlN* |
| 監視対象装置の生存確認、ネットワーク情報、操作ログの送信メールポート | set spy *targetN mlN* |
| 監視対象装置のログイン名、パスワード | set target-login-name<br>set target-login-password<br>set target-enable-password |
| 監視対象装置の生存確認機能を使用する | set target-check |
| 装置とネットワークに関する情報の送信時刻 | set network-info-time |
| 監視対象装置の操作ログをメールで送信する | set connect-log |
| **ユーザ定義の装置種別とフィルタ・スクリプトに関する設定項目** | |
| 装置種別のユーザ定義 | set user-target-type |
| ユーザ定義した装置固有のフィルタ | set target-filter |
| ユーザ定義した装置固有の操作スクリプト | set target-script |
| com ポートに対する装置種別の設定（デフォルトは "cisco"） | set target-type |

## RM-CM のポートとフィルタ・スクリプト

以下に、装置種別として “type_A”と“type_B”をユーザ定義し、COM1 と COM2 を“typeA”、COM3 を“typeB” に設定した場合の各ポートと「装置種別」「フィルタ」「スクリプト」の関連を示します。この図では、COM1 への入力をメールポート 1（ml1）に接続して送信する例を示しています。*comN*、*targetN*、rmc の各ポートへの入力情報に注意して、適切なメールポートとの接続を設定してください。フィルタ・スクリプトのユーザ定義に関する詳細は、後述します。

## 14.4 多機種対応用フィルタ・スクリプトの利用

RM-CM ソフトウェア Version2.1 以上をご使用の場合、ルートレックのホームページ上で提供されるフィルタ・スクリプトのデフォルト設定用ファイルを利用することができます。この設定ファイルは、特定の装置に対応した「装置種別」「フィルタ」「スクリプト」のデフォルト設定を提供するもので、ルートレックのホームページ（http://www.routrek.co.jp）からダウンロードしてご利用いただけます。

この設定ファイルを利用した場合、装置種別のユーザ定義やフィルタ・スクリプトの新規作成を行う必要はありません。また、提供されたフィルタやスクリプトの定義を任意に変更して利用することも可能です。弊社ホームページをご参照いただき、必要なファイルとドキュメントをダウンロードしてご活用ください。

# 15. ユーザ定義フィルタの作成

## 15.1　フィルタの作成と設定

監視対象装置からの出力情報を制御するためのフィルタは、装置の種別ごとに 0 から 7（tfl0~tfl7）までが定義可能です。各装置のコンソールポートから出力されるメッセージの形式にしたがって設定を行ってください。フィルタの設定は、**set target-filter** コマンドを実行し、UNIX の awk プログラム形式で記述することによって行います。装置種別が "cisco" 以外の装置に対してフィルタを作成する場合は、あらかじめ装置種別の定義をしておく必要があります。

RMC Version3.5 からは、Cisco 以外の装置用フィルタ・スクリプトが最初から用意されています。詳細に関しては、「14. 一般機器の接続とフィルタ・スクリプト」をご参照ください。

### フィルタの設定例

| フィルタ記述 | 機能 |
|---|---|
| /link down/ | ″link　down″という文字列を含む行を送信 |
| $0 !~ /link up/ | ″link　up″という文字列を含まない行を送信 |
| /[A-Za-z]+[0-3]/ | アルファベットで構成される単語に続いて<br>0 から 3 の 1 桁の数字を含む行を送信 |
| /error/<br>/warning/ | "error" または "warnig" 文字列を含む行を送信 |
| /Error/ {<br>　if ( $0 !~ /password/ ){<br>　　print<br>　}<br>} | "Error"の文字列を含み、かつ"password"を含まない行を送信 |

各々の監視対象装置（COM ポート）に対して使用されるフィルタとメールポートの関連は、**set spy** コマンドによって設定します。

以下に、COM1 に接続された装置の種別を "typeA" としてユーザ定義し、フィルタ tfl0 を作成してメールポート ml1 からの送信に利用する例を示します。

```
rmc@myrmc>enable
password:
[rmc@myrmc]# set  user-target-type  typeA          ← 装置種別 ”typeA” を定義
[rmc@myrmc]# set  target-filter  typeA  tfl0       ← typeA 用フィルタとして tfl0 を定義
[rmc@myrmc]# set  port  com1                       ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set  target-type  typeA         ← com1 ポートの装置種別を typeA
                                                     に設定
[rmc@myrmc(com1)]# set  port  ml1                  ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set  mailto  foo@routrek.co.jp   ← ml1 のメールアドレスを設定
[rmc@myrmc(ml1)]# set  spy  com1  tfl0  ml1        ← com1 に接続されるメールポートと
                                                     フィルタを指定
[rmc@myrmc(ml1)]# set  mail-service                ← メールサービスの開始
[rmc@myrmc(ml1)]# disable
rmc@myrmc>
```

以下の場合、該当 COM ポートに対するメッセージのフィルタリング処理は、一時的に停止されます。

- connect コマンドによる装置の手動操作中
- スクリプトの実行中(RM-CM が装置にコマンドを投入中)

## 15.2 フィルタ設定の確認テスト

ユーザ定義のフィルタが正しく設定されたかどうかは、**filter-test** コマンドによってあらかじめ確認することができます。

以下に、装置種別 ”typeA” のフィルタ tfl0 の設定を確認する場合の操作を示します。

```
rmc@myrmc>enable
password:
[rmc@myrmc]# filter-test  typeA  tfl0   ← typeA 装置のフィルタ tfl0 のテストを開始
XXXXXXXXXXXXXXXX                        ← テスト文字列（XX…X）入力後 Enter キーを押す
>XXXXXXXXXXXXXXXX                       ← 入力文字列がフィルタ設定に一致した場合は、
                                          入力文字列が表示される
  ______________________
                                        ← 入力文字列がフィルタ設定に一致しない場合
                                          フィルタ後の文字列は表示されない
                                        ← Ctrl－D を押してコマンド終了
[rmc@myrmc]# disable
rmc@myrmc>
```

Cisco 製品用に定義されたフィルタ tfl1（Severity Levels が 0 から 2 のメッセージを抽出）を指定した場合、filter-test コマンド実行時の表示は、次のようになります。

① Level 1 に相当するメッセージをテスト文字列として入力した場合

Feb 9 18:18:22.676: %PIM-1-INVALID_RP_JOIN: ← 入力文字列
>Feb 9 18:18:22.676: %PIM-1-INVALID_RP_JOIN: ← 表示

② Level 5 に相当するメッセージをテスト文字列として入力した場合

Feb 9 18:18:22.676: %AUTORP-5-MAPPING: ← 入力文字列

上記②では、テスト文字列がフィルタに一致しないため、何も表示されません。

# 16. ユーザ定義スクリプトの作成

本章では、一般機器を接続して「装置の生存確認」「装置情報の自動取得」「RMS からのコマンド発行」の機能を実行するスクリプトの作成とこれを利用するための設定について説明します。作成するスクリプトは、下記の 4 種類です。

- login スクリプト　　　　：装置にログインする際に必要な操作を記述します
- command スクリプト　　：装置にコマンドを発行する際に必要な操作を記述します
- target-check スクリプト：装置が作動中であるか否かの判断に必要な操作を記述します
- network-info スクリプト：装置からの情報収集時に実行すべきコマンドを記述します

RMC Version3.5 からは、Cisco 以外の装置用フィルタ・スクリプトが最初から用意されています。詳細に関しては、「14. 一般機器の接続とフィルタ・スクリプト」をご参照ください。

## 16.1 スクリプトの記述

### コマンドリスト

RM-CM の動作を定義するスクリプトは、下記のコマンドを使用して記述します。

| コマンド | 機能 |
|---|---|
| **!** | 外部コマンドを実行する |
| **break** | expect コマンドから抜ける |
| **call** | 他のスクリプトを呼び出して実行する |
| **dec** | 指定した変数から 1 を減算する |
| **exit** | スクリプトを終了する |
| **expect** | 装置からの入力を監視し、入力文字列に従ってコマンドを実行する |
| **gosub** | 指定したラベルの行のサブルーチンを実行する |
| **goto** | 指定したラベルの行にジャンプする |
| **if** | 条件式が正しい場合、指定したコマンドを実行する |
| **inc** | 指定した変数に 1 を加算する |
| **print** | スクリプト実行結果メールの本文中に、指定の文字列を挿入する |
| **return** | サブルーチンの実行を終了する |
| **send** | 指定した文字列＋キャリッジリターンを送信する |
| **set** | 変数に値を代入する |
| **sleep** | 指定秒数分、スクリプトの実行を停止する |
| **timeout** | スクリプト実行時間のタイムアウト値を指定する |
| **verbose** | COM ポートからの入力をメール本文に挿入するか否かを指定する |

### コメント行の記述

‘#’ から始まる行は、コメントとして解釈されます。

## 16.2 コマンドの機能

| **send <文字列>** | 指定した文字列および '¥r' (キャリッジリターン文字)を送信します。 |
|---|---|

文字列は以下のように指定します:

- 'send hello' のように、文字列をそのまま記述
- 'send "hello world"' のように、文字列をダブルクオートで囲んで記述

文字列中には、次のエスケープシーケンスおよび環境変数を記述することができます。

**エスケープシーケンスの記述**

send コマンドで指定可能な文字列は、次の通りです：

**¥n** ー 改行文字
**¥r** ー キャリッジリターン文字
**¥a** ー ビープ
**¥b** ー バックスペース文字
**¥c** ー デフォルトでは送信される'¥r'（キャリッジリターン文字）を抑制
**¥f** ー フォームフィード
**¥ddd** ー 8 進数(ddd)で指定したコード値の文字

上記以外の 1 文字を ¥ の後に記述した場合は、通常の文字と同様に処理されます。(たとえば、 '¥e' は 'e' と同じ扱いになります)

**環境変数の記述**

文字列として $(環境変数) を記述すると、環境変数に含まれる文字列が送信されます。利用可能な環境変数は以下の通りです：

**TARGET_LOGIN_NAME**
"set target-login-name" で指定された装置へのログイン名

**TARGET_LOGIN_PASSWORD**
"set target-login-password" で指定された装置へのログインパスワード

**TARGET_ENABLE_PASSWORD**
"set target-enable-password" で指定された装置への特権パスワード

**ARG1,ARG2,ARG3,ARG4**
"set target-type {target_type} [arg1] [arg2] [arg3] [arg4]"で指定された引数

**PORT**
カレント COM ポート名 (例: com1,com2,...)

**TARGET_TYPE**
"set target-type" で指定された装置種別名

**TARGET_SCRIPT**
実行中のスクリプト名 ("command","login","network-info","target-check")

**DESCRIPTION**
"set description" で指定された文字列

| **print <文字列>** | スクリプトの実行結果メールの本文中に、指定した文字列を挿入します。 |
|---|---|

文字列には send コマンドと同様、エスケープシーケンスや $（環境変数）の指定が可能です。対象となるメールサブジェクトは以下の通りです。

"Network information" (ネットワーク情報取得結果)
"Target command result" (定石コマンド実行結果)
"Target not respond", "target responds" (装置の生存確認結果)

| **<ラベル名>:** | goto, gosub で使用されるラベル名を定義します。 |
|---|---|

| **goto <ラベル名>** | 指定したラベルのある行にジャンプします。 |
|---|---|

| **gosub <ラベル名>** | 指定したラベルのある行をサブルーチンとして実行します。 |
|---|---|

サブルーチン中で return を実行すると、gosub の次の行から実行が再開されます。
なお、gosub はネスト可能です。

| **return** | サブルーチンの実行を終了します。 |
|---|---|

| **! <外部コマンド名>** | 外部コマンドを実行します。 |
|---|---|

コマンドの実行ステータスは変数 '$?' に格納されます。
(通常 0 で正常終了，非 0 でエラー)

実行可能な外部コマンドは、以下の通りです:

**sendcmd**

command スクリプトで使用されます。
'! sendcmd'を実行する度に、network-info スクリプトに記述された装置コマンドや、定石コマンドのように RMS から要求された装置コマンドが 1 行ずつ順に装置に送信されます。
set network-info-time の設定に基づく定期的装置情報取得の実行時には、network-info スクリプトで定義されたコマンドが送信されます。RMS からのコマンド発行要求時には、RMS で定義されたコマンドが送信されます。送信するコマンドがもう無い場合は、戻り値に 1 を返します。

**test**

Unix の test コマンドを実行します。

例：(set target-login-name が指定されているかどうかのチェック)

```
! test "$TARGET_LOGIN_NAME"
if $? = 0 goto has_login_name
```

| exit [戻り値] | スクリプトを終了します。 |
|---|---|

戻り値を省略した場合は exit 0 と同じ動作です。
スクリプトの実行状態に応じて、以下の戻り値を適切に設定する必要があります。

0： 正常終了
1： エラー(装置無応答等)
2： スクリプトエラー
3： パスワードエラー

| set <変数名> <値> | 変数に値を代入します。 |
|---|---|

変数名は a～z の英字 1 字が利用可能です。
変数に代入できる値は、整数または他の変数です。

| inc <変数名> | 指定した変数の値を 1 増やします。 |
|---|---|

| dec <変数名> | 指定した変数の値を 1 減らします。 |
|---|---|

| if <式> <コマンド> | 式が正しい場合、指定されたコマンドを実行します。 |
|---|---|

式は"<値> <演算子> <値>"の形をとり、値は整数または変数、演算子は <, >, !=(不等号), = の 4 種類が指定可能です。

例:

```
if a > 3 exit 1
```

| timeout <秒数> | スクリプト実行時間のタイムアウト値を指定します。 |
|---|---|

デフォルトのタイムアウト値は 120 秒です。それ以上時間がかかる処理を行う場合は、本コマンドで適切なタイムアウト値をセットしてください。

なお、後述する expect コマンド内でのタイムアウト指定と、本コマンドでのタイムアウト指定はそれぞれ独立しており、関連はありません。

| verbose <on\|off> | on にした場合、COM ポートからの入力文字列をメール本文に挿入します。 |
|---|---|

デフォルトの設定値はスクリプトごとに異なります：

| | |
|---|---|
| command | : on |
| login | : on |
| network-info | : on |
| target-check | : off |

| **sleep <秒数>** | 指定した秒数分、スクリプトの実行を一時停止します。 |
|---|---|

変数名は a～z の英字 1 字が利用可能です。
変数に代入できる値は、整数または他の変数です。

| **expect {**<br>**文字列 ［コマンド］**<br>**文字列 ［コマンド］**<br>**[timeout <秒数> [コマンド] ]**<br>**....**<br>**}** | 装置からの入力を監視し、入力された文字列に従ってコマンドを実行します。 |
|---|---|

装置からの入力を監視し、スクリプトに記述された文字列が入力される、もしくはタイムアウトが発生するまで、装置からの入力を続けます。該当する文字列が入力された場合は指定されたコマンドを実行します。コマンドを指定しなかった場合、expect {} の次の行が実行されます。

文字列には send コマンドと同様、エスケープシーケンスや $(環境変数)の指定が可能です。

デフォルトでは、expect の実行は 60 秒でタイムアウトし、スクリプトの実行が終了します。timeout の指定をすることにより、タイムアウト値、およびタイムアウト時に実行するコマンドの設定が可能です。なお、expect コマンドはネストできません。

expect {} 中に文字列が指定されていない場合、任意の文字が入力された時点で expect {} の次の行が実行されます。

例: （２秒間の未入力期間があるまで expect の実行を繰り返します。）

```
loop:
expect {
    timeout 2 goto no_input_for_2sec
}
goto loop
```

| **break** | expect コマンドを抜けだし、expect {} の次の行を実行します。 |
|---|---|

| **call <スクリプト名>** | 他のスクリプトを実行します。 |
|---|---|

スクリプトの実行が正常終了した場合は、元のスクリプトが引き続き実行されます。

通常、command スクリプトや target-check スクリプトから login スクリプトを呼び出す際に使用されます。

なお、expect コマンド中では、call コマンドは実行できません。

# 16.3　装置操作用スクリプトの作成

## 装置種別のユーザ定義

各スクリプトの定義に先立って、**set user-target-type** コマンドで装置種別を定義します。以降の *comN* ポートに対する装置種別の定義や各スクリプトの設定コマンド実行時は、ここで定義した装置種別を指定してください。

以下に、装置種別 “unix_server” をユーザ定義し、COM1 にこの装置種別を設定する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set  user-target-type  unix_server  ← 装置種別 ”unix_server” を定義
[rmc@myrmc]# set  port  com1
[rmc@myrmc(com1)]# set  target-type  unix_server       ← com1 の装置種別を
                                                          ”unix_server”に設定
[rmc@myrmc(com1)]#
```

## login スクリプト ： ログイン処理

login スクリプトは、**set target-script {*target_type*} login** で定義し、装置へのログイン操作を記述します。

このスクリプトは単独で実行されることはなく、ログイン動作を実行する他のスクリプトから呼び出して実行されます。したがって必須のスクリプトではありませんが、このスクリプトの定義によって、ログイン時の動作をコマンド発行要求のシーケンスとは独立して記述し、共通に利用することができます。

以下に、装置種別 “unix_server” として定義された UNIX サーバを COM1 に接続する場合のログインスクリプト記述例を示します。

このスクリプト例では、RM-CM に装置のログイン名が設定されている場合はこのログイン名を使用し、設定されていない場合には “root” でログインしています。装置のログインパスワードも、RM-CM の設定情報を使用しています（推奨）。これにより、装置固有の情報をスクリプト記述とは独立して管理することが可能になります。

login スクリプト記述例　　（ 内がスクリプト記述部分）

```
set  port  com1
set  target-type  unix_server                com1 ポートの装置種別を ”unix_server” に設定
set  target-login-name  {username}           com1 に接続された装置のログインユーザ名を設定
set  target-login-password  {password}       com1 に接続された装置のパスワードを設定

set  target-script  unix_server  login       ＜login スクリプトの設定コマンド実行＞
# send  [enter] and wait login prompt.
send ""                                      ＊キャリッジリターンを送信してプロンプトの受信待ち＊
expect  {
   "$ " exit 0                               $、または#が受信された場合は正常終結
   "# " exit 0
   "login:"  goto  login                     ログインプロンプトが受信された場合は、ログイン処理へ
   timeout  10  break                        10 秒間無応答の場合もログイン処理へ
}

# send  login  nam  (even if there is no response (getty -n))
login:                                       ＊ログイン処理の実行＊
! test "$TARGET_LOGIN_NAME"                  装置ログイン名が設定されているか否かのチェック
if $? = 0  send  $(TARGET_LOGIN_NAME)        設定されている場合は、ログイン名を送信
if $? != 0  send  "root"                     設定されていない場合は、”root” を送信
expect {                                     プロンプト文字列の受信待ち
   "$ " exit 0                               $、または#が受信された場合は正常終結
   "# " exit 0
   "assword:"  goto  password                パスワード要求が受信された場合は、パスワード処理へ
   timeout  10  goto  error                  10 秒間無応答の場合は、戻り値を 1 として異常終結
}
# send  password
password:                                    ＊パスワード送信処理の実行＊
send  $(TARGET_LOGIN_PASSWORD)               RMC に設定されたログインパスワードを送信
expect {                                     パスワード送信後のプロンプト待ち
   "$ " exit 0                               $、または#が受信された場合は正常終結
   "# " exit 0
   "incorrect"  goto  password_error         “incorrect” 受信時は、戻り値を 3 として異常終結
   timeout  10  goto  error                  10 秒間無応答の場合は、戻り値を 1 として異常終結
}
password_error:
exit 3
error:
exit 1
```

## command スクリプト ： 装置へのコマンド発行

command スクリプトは、装置に対するコマンド発行時の操作を定義するスクリプトです。このスクリプトは、**set target-script {*target_type*} command** で作成し、監視対象装置からの定期的情報取得時、および RMS からのコマンド発行要求時に実行されます。

command スクリプト内の ！sendcmd 実行時に発行されるコマンドは、network-info スクリプト、RMS の定石コマンドメニュー、インシデント発生時のコマンドとして定義します。

command スクリプトの実行によって装置から取得された情報は、*comN* ポートと *tragetN* ポートに入力されますが、*comN* ポートからの送信情報に関しては、フィルタ機能により抑制することができます。

次ページに、Unix サーバ（target-type “unix_server”）に対してコマンドを発行する場合のスクリプト記述例を示します。この例ではタイムアウト値が 240 秒に設定されています。実行完了に時間のかかるコマンド発行を要求する場合は、タイムアウトが発生しないように適正値を設定してください。

**RMS からのコマンド発行要求**

「定石コマンド発行」や「インシデント発生時のコマンド発行」のように、RMS から装置に対するコマンド発行が必要な処理が要求されると、RM-CM は command スクリプトを実行します。

RMS からのコマンド発行要求時に装置に対して発行されるコマンドは、RMS 側で定義されます。RMS の設定に関しては、下記のマニュアルをご参照ください。

・定石コマンドメニューの作成

➡「RMS ユーザーズ･ガイド 付録 3. ◇　定石コマンドメニューの作成」

・インシデント発生時のコマンド発行

➡「RMS ユーザーズ･ガイド ～管理者編～ 5.2 監視対象装置の登録情報」

command スクリプト記述例　　　（  内がスクリプト記述部分）

```
set  target-script  unix_server  command   ＜command スクリプトの設定コマンド実行＞
# command  script  for  Unix
call  login                                  ＊ログインスクリプトの実行＊
                                               （ログイン正常終了後は以下の処理へ）
timeout  240                                   スクリプト実行時間のタイムアウト値を設定

# command  loop                              ＊コマンド発行処理の実行＊
loop:
# send  a  command  one  by  one             ＊定義されたコマンドの発行処理
! sendcmd                                      外部コマンドとして sendcmd を実行
                                               （装置に対してコマンドを送信）
if $? != 0  goto  logout                       戻り値が 1（実行コマンド無し）であれば、ログアウトへ
gosub  wait_prompt                             プロンプト（コマンドの実行完了）待ち
goto  loop                                     次のコマンド発行処理へ

wait_prompt:                                 ＊プロンプト待ち処理＊
expect {                                       プロンプト文字列の受信待ち
  "$ " goto  wait_interval                     ＄、または＃が受信された場合は wait_interval へ
  "# " goto  wait_interval
  "assword:" goto  sudo_password               パスワード要求が受信された場合、パスワード処理へ
  timeout  120  goto  error                    120 秒間無応答の場合は、異常終結
}
# wait  2  sec  interval  to  confirm  prompt
wait_interval:                               ＊コマンド実行完了確認
expect {                                       （2 秒間の無応答が発生するまでループ）
  timeout  2  return                            2 秒間無応答であれば、サブルーチンの実行終了
}
goto  wait_interval                            再度、2 秒間の無応答待ちへ
sudo_password:                               ＊パスワード処理＊
send  $(TARGET_LOGIN_PASSWORD)                 RMC に設定された装置のログインパスワードを送信
goto  wait_prompt                                          プロンプト待ちへ
logout:                                      ＊ログアウト処理＊
send  "logout"                                 logout  文字列を送信
expect {                                       ログインプロンプト待ち
  "login:" exit 0                              login:  文字列が受信された場合は、正常終結
  timeout  20  goto  error                                 20 秒間無応答の場合は、異常終結
}
error:
exit 1
```

## target-check スクリプト ： 装置の生存確認

装置の稼動状態を判断するために、RM-CM は次の 2 通りの確認方法を用意しています。

### ● RS232C の信号線ステータスによる確認

RS232C の DSR（Data Se Ready）信号によって装置の生存確認を行います。この場合、target-check スクリプトの定義は必要ありません。target-check スクリプトが定義されていない装置に対して生存確認を行う設定（set target-check）をした場合、RM-CM は RS-232C シグナルによって装置の状態を確認し、DSR が ON であれば、装置は正常に稼動中と判断します。

以下に、COM1 に接続された装置（target_type "unix_server"）に対して、信号線ステータスによる生存確認を行い、結果をメールポート ml1 に指定した宛先に、通知する場合の必要な設定を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set user-target-type “unix_server” ← 装置種別の定義
[rmc@myrmc]# set port com1                     ← カレントポートを comN に設定
[rmc@myrmc(com1)]# set target-type “unix_server”  ← 装置種別を“target-type”に
                                                   設定
[rmc@myrmc(com1)]# set target-check            ← 監視対象装置の生存確認を設定
[rmc@myrmc(com1)]# set spy target1 ml1         ← 生存確認送信先ﾒｰﾙﾎﾟｰﾄを設定
[rmc@myrmc(com1]# show port com1               ← com1 の設定を確認
[rmc@myrmc(com1)]#
```

この方法は、コマンドによる設定のみで実行できるため簡易ですが、信号線の状態によって装置の稼動状態を判断するため、装置がハングアップしている場合の異常検出など、ソフトウェアレベルの稼動状態は確認できません。

### ● 装置の操作による応答確認： target-check スクリプトの利用

target-check スクリプトに装置に対する操作と期待する応答を記述し、スクリプトの実行結果によって装置の状態を判断します。

target-check スクリプトは **set target-script {*target_type*} target-check** コマンドで作成し、set target-check コマンドで設定された時間間隔で実行されます。スクリプトの実行結果は、"Target not respond", “Target responds”というサブジェクトのメールで、*targetN* ポートに接続されたメールポートから送信されます。

以下に、COM1 に接続された UNIX サーバを監視する場合の target-check スクリプト記述例を示します。この例では、UNIX コンソールにキャリッジリターンを送信し、プロンプト（"$"、"#"、もしくは "login:"）が 20 秒以内に応答されるか否かで装置の状態を判断しています。

target-check スクリプト記述例　　（  内がスクリプト記述部分）

```
set  user-target-type  unix_server               装置種別 ”unix_server” を定義
set  port  com1
set  target-type  unix_server                    com1 ポートの装置種別を ”unix_server” に設定
set  target-check  10                            10 分間隔で装置の生存確認を実行にする
set  spy  target1  ml1                           生存確認結果の送付先をメールポート 1 に設定

set  target-script  unix_server  target-check    <target-check スクリプトの設定コマンド実行>
send  “”                                         ＊キャリッジリターンを送信してプロンプト待ち＊
expect  {                                        プロンプト待ちの記述
     “$” exit 0                                  $,、#、または login: を受信した場合は、正常終結
     “#” exit 0
     “login:” exit 0
     timeout  20  exit 1                         20 秒間無応答であれば、異常終結
}
```

RM-CM はスクリプト実行後の戻り値で装置状態を確認し、戻り値 ＝1 の場合には、装置
が無応答であると判断して ”Target not respond” のサブジェクトのメールを送信します。戻り値を正しく設定するようにご注意ください。

## network-info スクリプト：装置からの情報取得

network-info スクリプトは、COM ポートに接続された装置からの情報取得に必要なコマンドを定義します。このスクリプトは、**set target-script {*target_type*} network-info** コマンドで作成します。network-info スクリプトは、command スクリプトに記述された ! sendcmd の実行時に参照され、記述されたコマンドが 1 行ずつ装置に送信されます。

装置情報収集のための command スクリプトは、set network-info-time コマンドによって設定された時刻に実行されます。スクリプトの実行結果として得られた監視対象装置からの情報（出力結果）は、”Network information” というサブジェクトのメールで *targetN* ポートに接続されたメールポートから送信されます。

以下に、COM2 に接続された Unix サーバに対して 0 時と 12 時の 2 回自動情報取得を実行し、その結果を ml0 と ml1 に設定された宛先に送信する場合の設定例を示します。

このスクリプトでは、情報取得用コマンドとして、last、netstat、ps の 3 コマンドを定義していますが、コマンド発行の処理自体は command スクリプトと login スクリプトに記述しているため、network-info スクリプトには、装置に対して送信すべきコマンドシーケンスのみを記述します。また、装置のログイン名とログインパスワードに設定された情報は、login

スクリプト実行時に使用されます。

network-info スクリプト記述例　（  内がスクリプト記述部分）

```
set  port  com2
set  target-type  unix_server                装置種別”unix_server”を定義
set  target-login-name  admin                com2 に接続された装置のログイン名を設定
set  target-login-password  password         com2 に接続された装置のログインパスワードを設定
set  network-info-time  0,12 0               装置情報取得の時刻を設定
set  spy  target2  ml0                       装置情報取得結果をメールポート 0 から送信
set  spy  target2  ml1                       装置情報取得結果をメールポート 1 から送信

set  target-script  unix_server  network-info    <network-info スクリプトの設定コマンド実行＞
# network  information  command  for  Unix
last                                          過去のブート、シャットダウン、ログインの記録表示コマンド
netstat                                       ネットワーク状況の表示コマンド
ps afxw                                       実行中のプロセス状態表示コマンド
```

**network-info スクリプト中の操作用スクリプト記述**

network-info スクリプト中に、装置に対する実行コマンドではなく、command スクリプトなどと同様の操作用スクリプトを記述したい場合は、スクリプトの先頭行に下記の記述を行います。
この記述を行った場合、以後の行は、装置に発行するコマンドではなくスクリプトとして処理されます。

**#script**

この記述は、network-info スクリプトの先頭行でのみ有効です。また、この記述を行った場合、#script 以下の行に装置のコマンドを記述することはできませんのでご注意ください。
なお、network-info 以外のスクリプト、および RMS で定義される装置へのコマンド定義行にこの記述を行った場合は、コメント行として扱われます。

network-info コマンドに関しては、➡「RM-CM クイックリファレンス」をご参照ください。

## 16.4　スクリプトのデバッグ方法

**script-test** ***com*** ***{スクリプト名}*** コマンドを実行することにより、スクリプトを手動で実行して入出力の内容をターミナルに表示し、実行結果を確認することができます。

script-test コマンド実行時は、予めテストする COM ポートに装置種別を設定しておく必要があります。なお、script-test コマンドは、装置種別が ”cisco” （デフォルト種別）に設定されているポートに対しては実行できませんのでご注意ください。

以下に、COM1 に設定された command スクリプトをデバッグモードで実行した場合の出力例（一部）を示します。command スクリプトは、network-info スクリプトなどの記述を参照して実行されるため、デバッグモードで実行した場合は、スクリプト実行前に、発行すべきコマンドの入力が要求されます。

command スクリプトデバッグ例　（ 内がスクリプト実行部分）

```
[rmc@myrmc]# script-test  com1  command
enter  test  commands.                          ＊発行するコマンドの入力要求＊
to  start  the  script  press  CTRL-D  at  the  beginning  of  line.
ps                                              ps をキーボードから入力、改行後 CTRL-D を入力

<1: call  login>                                ＊login スクリプトの実行開始＊
<1: send "">
<2: expect  {>
login: <3: "login: "  goto  login>                 login:を受信し、login: へ
<7: }>
<10: ! test  "$TARGET_LOGIN_NAME">                 装置ログイン名の定義をチェック
<11: if $? = 0  send  $(TARGET_LOGIN_NAME)>
<11: if $? = 0  send  $(TARGET_LOGIN_NAME)>
<12: if $? != 0  send  "root">
<13: expect {>
server_1                                           RMC に設定されたログイン名を送信
Password:<16: "assword:"  goto  password>
<18: }>
<21: send  $(TARGET_LOGIN_PASSWORD)>
<22: expect  {>
$ <23: "$ " exit 0>                                プロンプトの確認
<27: }>                                            login スクリプトの実行終了
<2: timeout  240>
<5: ! sendcmd>                                     装置に対するコマンド発行
ps                                                 ps  を送信
---start command result---
---ps---
<6: if $? != 0  goto  logout>
<7: gosub  wait_prompt>
<11: expect {>
 [ ・・・・・ コマンド実行結果の出力内容 ・・・・・   以下省略 ]
```

## 16.5　一般機器に対する COM ポートの設定

以下に、監視対象装置の種別とフィルタ・スクリプトを新たにユーザ定義して、これを利用する場合に必要となるコマンドの実行シーケンスを示します。必要な設定項目を確認して、正しい設定を行ってください。

フィルタのユーザ定義に関しては、➡「15. ユーザ定義フィルタの作成」をご参照ください。

```
rmc@myrmc > enable
password:

---- 装置種別ごとに必要な設定と設定の確認 ----
set  user-target-type  mytarget              ユーザ定義の装置種別 "mytarget" を設定
set  target-filter  mytarget  tflN           mytarget の tflN フィルタを設定
show  target-filter  mytarget                mytarget のフィルタ内容を表示
set  target-script  mytarget  login          mytarget の login スクリプトを設定
set  target-script  mytarget  command        mytarget の command スクリプトを設定
set  target-script  mytarget  network-info   mytarget の network-info スクリプトを設定
set  target-script  mytarget  target-check   mytarget の target-check スクリプトを設定
show  target-script  mytarget                mytarget に設定されたスクリプト内容を表示

---- 監視対象装置（COM ポート）ごとに必要な設定 ----
set  port  comN
set  target-type  mytarget                   装置の種別を "mytarget" に設定

set  target-login-name  xxxxx              ┐
set  target-login-password  xxxxx          │
set  target-check                          ├ 装置ごとの情報と RMC 機能の設定
set  network-info-time  h,m                │
set  connect-log                           ┘

set  spy  comN  tflN  mlN        comN に適用するフィルタと送信メールポートを設定
set  spy  targetN  mlN           生存確認・ネットワーク情報・操作ログの送信メールポートを設定

set  mail-service                            メールサービスの開始
disable
myrmc>
```

## 16.6 スクリプト作成上の注意点

### ログアウトの記述

スクリプトでログインを行った場合は、最後に必ずログアウトの記述を行ってください。

ログインした状態のままでスクリプトを終了した場合、スクリプトの側で記述を工夫しないと、次回のスクリプト実行でログイン処理がタイムアウトエラーになります（すでにログイン済みのため）。また、セキュリティ上も好ましくありません。

### パスワードの設定

スクリプト中にパスワード文字列を直接記述することは、なるべく避けてください。

環境変数 '"$(TARGET_LOGIN_PASWORD)"、または'"$(TARGET_ENABLE_PASSWORD)"をスクリプト中に記述することにより、set target-login-password,
set target-enable-password で設定したパスワード文字列を使用して装置にログインすることができます。

## 16.7 よくあるご質問

■ **スクリプトがタイムアウトエラーになってしまいます**

スクリプトでもっとも多いエラーが、タイムアウトエラーです。これは、期待する受信待ち文字列が得られなかった場合に発生します。
スクリプトをデバッグモードで手動実行し、(「16.4　スクリプトのデバッグ方法」参照)どの箇所でエラーが起きているかを調査して必要な対応を行ってください。

■ **装置側でのコマンド実行中にタイムアウトエラーが発生します**

タイムアウトの初期値は 120 秒になっています。コマンドの実行にそれ以上の時間がかかる場合は、あらかじめタイムアウト値を長めに設定してください。タイムアウトの設定はスクリプト中に "timeout <秒数>"と記述することで行います。

■ **スクリプト実行中に表示される文字列にフィルタ処理はできないのでしょうか**

RM-CM のフィルタは、COM ポートから送信される "Target Message" メールに対してのみ適用されます。スクリプト実行結果として送信される"Netowk-info"、"Target not respond"、"Target responds" の各メールに対しては適用されません。
但し、スクリプトの verbose コマンドを使用することで、入力された文字列をメール本文中に含めるかどうかを操作することは可能です。

# 17. 製品仕様

## 17.1　本体仕様

| 項目 | RM-CM1200 | RM-CM200 |
|---|---|---|
| インタフェース | シリアルポート EIA-RS232D (RJ-45) ×12 | シリアルポート EIA-RS232D (RJ-45) ×2 |
| | シリアルポート EIA-RS232D (DB9) ×2 | ―――― |
| ネットワークポート | IEEE802.3 10BASE-T/100BASE-TX (RJ-45) ×2 | IEEE802.3 10BASE-T (RJ-45) ×1 |
| 表示機能 | LCD 表示パネル | ステータス LED (7 セグメント), |
| | LINK/ACT LED , Speed LED | LINK/ACT LED |
| 電源 | 100V AC 50/60Hz | DC 5V<br>(AC アダプタ 定格入力 100V AC 50/60Hz) |
| 消費電力 | 1A (100V AC) | DC 5V 1A |
| 使用条件 | 気温 0～40℃ 湿度 15～85%<br>ただし結露しないこと | 気温 0～40℃ 湿度 15～85%<br>ただし結露しないこと |
| EMI | VCCI クラス A | VCCI クラス B |
| 外形寸法(WxDxH) | 441x310x43.5 (mm) | 85x110x23 (mm) |
| 重量 | 4.8Kg | 140g |

## 17.2　COM ポート仕様

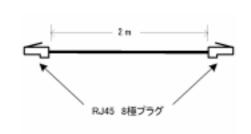
**COM1～COM12 シリアルポート ピン配置**

| ピン番号 | 信号 | 入出力 |
|---|---|---|
| 1 | RTS | OUT |
| 2 | DTR | OUT |
| 3 | TXD | OUT |
| 4 | SG | ― |
| 5 | SG | ― |
| 6 | RXD | IN |
| 7 | DSR | IN |
| 8 | CTS | IN |

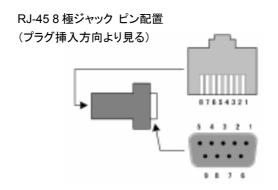
**COMA、COMB シリアルポート ピン配置 (RM-CM1200 のみ)**

| ピン番号 | 信号 | 入出力 |
|---|---|---|
| 1 | DCD | IN |
| 2 | RXD | IN |
| 3 | TXD | OUT |
| 4 | DTR | OUT |
| 5 | SG | ― |
| 6 | DSR | IN |
| 7 | RTS | OUT |
| 8 | CTS | IN |
| 9 | RI | IN |

# 17.3　付属ケーブル／コネクタ仕様

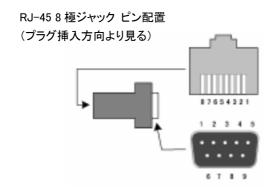
## RJ-45 ROLLED シリアルケーブル仕様 (クロス)

| RJ-45 | RJ-45 |
|---|---|
| 1 | 8 |
| 2 | 7 |
| 3 | 6 |
| 4 | 5 |
| 5 | 4 |
| 6 | 3 |
| 7 | 2 |
| 8 | 1 |

## RJ-45・DB9 ソケット変換コネクタ仕様（ストレート／シリアル端末接続用）

RJ-45 8 極ジャック ピン配置
（プラグ挿入方向より見る）

D-sub 9 極ソケット ピン配置
（プラグ挿入方向より見る）

| RJ-45 ジャック（メス） | 9 極ソケット（メス） | 信号 |
|---|---|---|
| 1 | 7 | CTS |
| 2 | 4 | DSR |
| 3 | 3 | RXD |
| 4 | 5 | GND |
| 5 | 5 | GND |
| 6 | 2 | TXD |
| 7 | 6 | DTR |
| 8 | 8 | RTS |

## RJ-45・DB9 プラグ変換コネクタ仕様（クロス／モデム接続用）

RJ-45 8 極ジャック ピン配置
（プラグ挿入方向より見る）

D-sub 25 極プラグ ピン配置
（ソケット挿入方向より見る）

| RJ-45 ジャック（メス） | 9 極プラグ（オス） | 信号 |
|---|---|---|
| 1 | 8 | CTS |
| 2 | 6 | DSR |
| 3 | 2 | RXD |
| 4 | 5 | GND |
| 5 | 5 | GND |
| 6 | 3 | TXD |
| 7 | 4 | DTR |
| 8 | 7 | RTS |

# 18. 商標とライセンス

## Open SSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)."

## Postfix mail system



## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991



GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1

   above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as

distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

   integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## net-snmp

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2001-2002, Networks Associates Technology, Inc

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this code are copyright (c) 2001-2002, Cambridge Broadband Ltd.

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# 製品に関するサポートのご案内

製品に関するお問い合わせやテクニカルサポートについては、下記の弊社サポートページをご覧ください。

**http://www.routrek.co.jp/support/**

また、製品に関する最新情報やマニュアルも上記ページからダウンロードすることができますのでご参照ください。



株式会社ルートレック･ネットワークス
〒213-0011 神奈川県川崎市高津区久本３－５－７ 新溝ノロビル
Tel. 044-829-4361　　Fax. 044-829-4362